Management Software

AT-S39

User's Guide

AT-8012M, AT-8016F/xx (SC or MT), AT-8024, AT-8024GB, AT-8024M, AT-8026FC, AT-8088/xx (SC or MT) FAST ETHERNET SWITCHES

VERSION 3.1.0

PN 613-50245-00 Rev H

Allied Telesyn

Simply connecting the IP world

Copyright © 2003 Allied Telesyn, Inc.
960 Stewart Drive Suite B, Sunnyvale, CA 94085 USA

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Microsoft is a registered trademark of Microsoft Corporation, Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

List of Figures 9

Preface 12
How This Guide is Organized 12
Document Conventions 14
Where to Find Web-based Guides 15
Contacting Allied Telesyn 16
Sales or Corporate Information 16
Management Software Updates 17

Section I
Overview 18

Chapter 1

Overview 19
Local Management Session 21
Telnet Management Session 22
Web Browser Management Session 23
SNMP Management Session 24
Management Access Levels 25

Section II
Local and Telnet Management 26

Chapter 2

Starting a Local or Telnet Management Session 28
Local Management Session 29
Starting a Local Management Session 30
Enhanced Stacking 33
Quitting from a Local Session 33
Telnet Management Session 34
Starting a Telnet Management Session 34
Quitting from a Telnet Management Session 35

Chapter 3

Basic Switch Parameters 36
When Does a Switch Need an IP Address? 37
How Do You Assign an IP Address? 38
Configuring an IP Address and Switch Name 39
Activating the BOOTP and DHCP Services 42
Configuring SNMP Community Strings and Trap IP Addresses 44
Resetting a Switch 47
Configuring the AT-S39 Software Security Features 48
Configuring the Management Passwords 48
Configuring Management Access 51
Viewing the AT-S39 Version Number and Switch MAC Address 52
Pinging a Remote System 53
Returning the AT-S39 Software to the Factory Default Values 54
Configuring the Console Startup Mode 55
Configuring BALUN Cable Detection 56

Chapter 4

Enhanced Stacking 57
Enhanced Stacking Overview 58
Guidelines 58
Setting a Switch's Enhanced Stacking Status 61
Selecting a Switch in an Enhanced Stack 63
Returning to the Master Switch 64

Chapter 5

Port Parameters 65
Displaying Port Status 66
Configuring Port Parameters 69
Displaying Uplink Information 73

Chapter 6

Port Security 75
Port Security Overview 76
Configuring Port Security 78
Configuring the Limited Security Mode 80

Chapter 7

Port Trunking 82
Port Trunking Overview 83
Load Distribution Methods 84
Creating a Port Trunk 89
Deleting a Port Trunk 91

Chapter 8

Port Mirroring 92
Port Mirroring Overview 93
Creating a Port Mirror 94
Deleting a Port Mirror 95

Chapter 9

STP and RSTP 96
STP and RSTP Overview 97
Bridge Priority and the Root Bridge 98
Mixed STP and RSTP Networks 104
Spanning Tree and VLANs 104

Enabling or Disabling STP or RSTP 105
Configuring STP 106
Configuring a Bridge's STP Settings 106
Configuring a Port's STP Settings 108
Configuring RSTP 110
Configuring a Bridge's RSTP Settings 110
Configuring a Port's RSTP Settings 112

Chapter 10

Virtual LANs Overview 115
AT-S39 Management Software Switch Modes 116
Setting the Switch Mode 117
Setting VLAN Status 118
VLAN Overview 119
Increased Performance 119
Improved Manageability 119
Increased Security 120
VLAN Modes 120
User-Configured VLANs 121
Port-based VLAN Overview 121
Tagged VLAN Overview 127
Multiple VLAN Mode Overview 132
802.1Q- Compliant Multiple VLANs mode 133
Non-802.1Q Compliant Multiple VLANs 135

Chapter 11

Configuring User-Created VLANs 137
Creating a New Port-based or Tagged VLAN 138
Creating a Port-based VLAN Example 142
Creating a Tagged VLAN Example 143
Modifying a VLAN 144
Displaying VLAN Information 147
Deleting a VLAN 148
Deleting All VLANs 150
Displaying PVIDs and Priorities 151
Enabling or Disabling Ingress Filtering 152
Designating a Management VLAN 154

Chapter 12

Multiple VLAN Configuration 156
Preserving User-Configured VLAN Definitions 157
Activating or Deactivating the Multiple VLAN Mode 158
Uplink VLANs - Multiple VLANs Mode Management 159
Displaying VLAN Information 160

Chapter 13

MAC Address Table 161
MAC Address Overview 162
Displaying MAC Addresses 164
Viewing MAC Addresses by Port 167
Identifying a Port Number by MAC Address 168
Viewing the MAC Addresses of a VLAN 169
Deleting All Dynamic MAC Addresses 170
Adding Static and Multicast MAC Addresses 171
Deleting MAC Addresses 172
Changing the Aging Time 173

Chapter 14

Class of Service 174
Class of Service Overview 175
Configuring CoS 176

Chapter 15

IGMP Snooping 177
IGMP Snooping Overview 178
Activating IGMP Snooping 180
Displaying a List of Host Nodes 183
Displaying a List of Multicast Routers 184

Chapter 16

Broadcast Storm Control 185
Broadcast Storm Control Overview 186
Configuring the Interval Timer 188
Configuring the Maximum Broadcast Frame Count 190

Chapter 17

TACACS+ and RADIUS Protocols 191
TACACS+ and RADIUS Overview 192
Configuring an Authentication Method 195

Chapter 18

802.1x Port-Based Network Access Control 200
Port Access Control Overview 201
Client 201
Switch 201
Authentication Server 201
Enabling and Disabling Port Access Control 203
Configuring Port Access Control Parameters 204
Viewing Port Access Status 207

Chapter 19

Ethernet Statistics 208
Displaying Port Statistics 209
Displaying Switch Statistics 211

Chapter 20

File Downloads and Uploads 213
Obtaining Software Updates 215
Transferring Files from a Local Management Session 216
Transferring Files from a Telnet Session 220
Downloading Files Switch to Switch 223
Uploading Files 225

Section III
Web Browser Management 226

Chapter 21

Starting a Web Browser Management Session 227
Starting a Web Browser Management Session 228
Browser Tools 229
Quitting from a Web Browser Management Session 230

Chapter 22

Basic Switch Parameters 231
Configuring an IP Address and Switch Name 232
Activating the BOOTP and DHCP Services 236
Viewing System Information 237
Configuring the SNMP Parameters and Trap IP Addresses 239
Resetting a Switch 241
Pinging a Remote System 242
Returning the AT-S39 Software to the Factory Default Values 243

Chapter 23

Enhanced Stacking 244
Setting a Switch's Enhanced Stacking Status 245
Selecting a Switch in an Enhanced Stack 247
Returning to the Master Switch 248

Chapter 24

Port Parameters 249
Configuring Port Parameters 250
Displaying Port Status and Statistics 253

Chapter 25

Port Security 258
Displaying the Port Security Level 259

Chapter 26

Port Trunks 260
Creating or Deleting a Port Trunk 261

Chapter 27

Port Mirroring 263
Creating or Deleting a Port Mirror 264

Chapter 28

STP and RSTP 266
Enabling or Disabling STP or RSTP 267
Configuring STP 268
Configuring RSTP 272
Displaying STP or RSTP Settings 276

Chapter 29

Virtual LANs 278
Creating A New Port-Based or Tagged VLAN 279
Modifying a Port-Based or Tagged VLAN 282
Deleting a Port-Based or Tagged VLAN 283
Displaying VLANs 284
Selecting a Multiple VLANs Mode 285
Setting the Switch's Mode 287
Enabling or Disabling VLANs 288

Chapter 30

MAC Address Table 289
Viewing the MAC Address Table 290
Adding Static and Multicast MAC Addresses 293
Deleting MAC Addresses 294
Changing the Aging Time 295

Chapter 31

Class of Service 296
Configuring CoS 297

Chapter 32

IGMP Snooping 298
Configuring IGMP Snooping 299
Displaying a List of Host Nodes and Multicast Routers 302

Chapter 33

Broadcast Storm Control 304
Configuring the Interval Timer 305
Setting the Maximum Number of Broadcast Frames 306

Chapter 34

TACACS+ and RADIUS Protocols 307
Configuring TACACS+ and RADIUS 308

Appendix A

AT-S39 Default Settings 312

Index **316**

List of Figures

Figure 1: Connecting a Terminal or PC to the RS232 Terminal Port 30
Figure 2: Main Menu 32
Figure 3: Administration Menu 39
Figure 4: System Configuration Menu 44
Figure 5: Advanced Configuration Menu 45
Figure 6: SNMP Configuration Menu 45
Figure 7: Passwords Menu 49
Figure 8: Diagnostics Menu 52
Figure 9: Enhanced Stacking Example 60
Figure 10: Enhanced Stacking Menu 61
Figure 11: Stacking Services Menu 63
Figure 12: Port Menu 66
Figure 13: Port Status Window 67
Figure 14: Port Configuration Menu 69
Figure 15: Uplink Information Menu 73
Figure 16: GBIC Information Menu 74
Figure 17: Port Security Menu 78
Figure 18: Limited Security Mode Menu 80
Figure 19: Port Trunk Example 83
Figure 20: Load Distribution Method 85
Figure 21: Port Trunking Menu 89
Figure 22: Port Trunking Menu 94
Figure 23: Point-to-Point Ports 102
Figure 24: Edge Port 103
Figure 25: Point-to-Point and Edge Point 103
Figure 26: VLAN Fragmentation 104
Figure 27: Spanning Tree Menu 105
Figure 28: STP Menu 106
Figure 29: Config STP Port Settings Menu 108
Figure 30: RSTP Menu 110
Figure 31: RSTP Port Parameters 112
Figure 32: Configure RSTP Port Settings Menu 113
Figure 33: Port-based VLAN - Example 1 124
Figure 34: Port-based VLAN - Example 2 126
Figure 35: Example of a Tagged VLAN 130
Figure 36: VLAN Menu 138
Figure 37: Configure VLANs Menu 139

Figure 38: Create VLAN Menu 139
Figure 39: Modifying a VLAN Menu 144
Figure 40: Show VLANs Menu - User Configured 147
Figure 41: Delete a VLAN Menu 148
Figure 42: Show PVIDs and Priorities Window 151
Figure 43: Show VLANs Window -Multiple VLAN 160
Figure 44: MAC Address Table Menu 164
Figure 45: Show All MAC Addresses Window 165
Figure 46: IGMP Snooping Configuration Menu 180
Figure 47: View Multicast Hosts List Window 183
Figure 48: View Multicast Routers List Window 184
Figure 49: Broadcast Storm Control Menu 188
Figure 50: Authentication Menu 195
Figure 51: Authentication Menu (TACACS+) 196
Figure 52: RADIUS Client Configuration 198
Figure 53: RADIUS Server Configuration 199
Figure 54: Port Access Control Menu 203
Figure 55: Configuring Port Access 204
Figure 56: Configure Port Access Parameters Menu 205
Figure 57: Display Port Access Status Menu 207
Figure 58: Ethernet Statistics Menu 209
Figure 59: Display Module Statistics Window 211
Figure 60: Downloads & Uploads Menu 217
Figure 61: Local Management Window 218
Figure 62: Send File Window 218
Figure 63: XModem File Send Window 219
Figure 64: Downloads & Uploads Menu 221
Figure 65: Entering a Switch's IP Address in the URL Field 228
Figure 66: Home Page 229
Figure 67: General Tab Menu - Configuration 233
Figure 68: General Tab Window - Monitoring 237
Figure 69: SNMP Tab 239
Figure 70: Ping Client Menu 242
Figure 71: Factory Default Tab 243
Figure 72: Enhanced Stacking Tab 246
Figure 73: Stacking Switches Menu 247
Figure 74: Port Setting Configuration Tab 250
Figure 75: Settings for Port Menu 251
Figure 76: Port Monitoring Page 253
Figure 77: Port Status Window 254
Figure 78: Port Statistics Window 256
Figure 79: Port Security Menu 259
Figure 80: Port Trunking Menu 261
Figure 81: Port Mirroring Menu 264
Figure 82: Spanning Tree Tab 267
Figure 83: STP Bridge Configuration Menu 268
Figure 84: STP Port Configuration Menu 270
Figure 85: RSTP Bridge Configuration Menu 272
Figure 86: RSTP Port Configuration Menu 274
Figure 87: Spanning Tree Tab - Monitoring 276
Figure 88: Rapid Spanning Tree Window - Monitoring 277
Figure 89: VLAN Menu 279
Figure 90: Add VLAN Menu 280
Figure 91: VLAN Monitoring Window 284
Figure 92: Multiple VLAN Configuration 285

Figure 93: Forwarding Database Tab 290
Figure 94: Add Static MAC Address Menu 293
Figure 95: IGMP Menu - Configuration 299
Figure 96: IGMP Window - Monitoring 302
Figure 97: Server-based Authentication Tab 308
Figure 98: TACACS+ Configuration Menu 309
Figure 99: RADIUS Configuration 310

Preface

This guide contains instructions on how to configure an AT-8000 Series Fast Ethernet Switch using the AT-S39 management software.

The AT-8000 Series consists of the following Fast Ethernet switches:

- ❑ AT-8012M
- ❑ AT-8016F/xx (SC or MT)
- ❑ AT-8024
- ❑ AT-8024GB
- ❑ AT-8024M
- ❑ AT-8026FC
- ❑ AT-8088/xx (SC or MT)

How This Guide is Organized

This manual is divided into three sections.

Section I: Overview

This section contains just one chapter. It reviews the different ways that you can access the AT-S39 management software on a switch.

Section II: Local and Telnet Management

The chapters in this section explain how to manage a switch from a local management session or a Telnet management session.

A local management session is established by connecting a terminal or PC to the RS-232 Terminal Port on the front panel of the switch.

A Telnet management session is established using the Telnet application protocol. This type of management session can be performed from any workstation on your network that has the application protocol.

Section III: Web Browser Management

The chapters in this section explain how to manage a switch using a web browser, such as Microsoft® Internet Explorer or Netscape® Navigator, from a workstation on your network.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in Portable Document Format (PDF) from on our web site at www.alliedtelesyn.com. You can view the documents on-line or download them onto a local workstation or server.

Contacting Allied Telesyn

To contact Technical Support by phone, find your country or region in the table below.

United States, Canada, Mexico, Central America, South America Tel: 1 800 428 4835 (option 4)	Germany, Switzerland, Austria, Eastern Europe Tel: (+49) 30-435-900-126
United Kingdom, Denmark, Norway, Sweden, Finland (+44) 1-235-442560	France, Belgium, Luxembourg, The Netherlands, Middle East, Africa (+33) 1-60-92-15-25
Singapore, Taiwan, Thailand, Malaysia, Indonesia, Korea, Philippines, China, India, Hong Kong Tel: (+65) 3815-612	Australia Tel:1 (800) 000-880
Italy, Spain, Portugal, Greece, Turkey, Israel Tel: (+39) 02-41-30-41	Japan Tel: (+81) 3-3443-5640

You can also contact Technical Support on-line at **http://kb.alliedtelesyn.com**.

Sales or Corporate Information

Allied Telesyn, Inc.
19800 North Creek Parkway,
Suite 200
Bothell, WA 98011
Tel:1 (425) 487-8880
Fax:1 (425) 489-9191

Management Software Updates

New releases of management software for our managed products are available from our web site at www.alliedtelesyn.com and our FTP server at ftp.alliedtelesyn.com. To use the FTP server, enter 'anonymous' for the user name when you log in and your e-mail address for the password.

Section I
Overview

This section provides a brief overview of the AT-S39 management software. It explains some of the functions that you can perform with the management software and reviews different methods for accessing the AT-S39 software on an AT-8000 Series Fast Ethernet Switch.

Chapter 1
Overview

The AT-S39 management software is intended for the AT-8000 Series Fast Ethernet Switches. The software is used to monitor and adjust a switch's operating parameters. Functions that you can perform with the software include:

- ❑ Enable and disable ports
- ❑ Configure port parameters, such as port speed and duplex mode
- ❑ Create virtual LANs (VLANs)
- ❑ Create port trunks and port mirrors
- ❑ Assign an Internet Protocol (IP) address and subnet mask
- ❑ Activate and configure the Spanning Tree Protocol (STP)
- ❑ Activate enhanced stacking functions
- ❑ Activate and configure RSTP
- ❑ Configure Class of Service (COS)
- ❑ Enable and configure IGMP snooping
- ❑ Enable and configure broadcast storm control
- ❑ Download and upload image and configuration files
- ❑ Configure port security
- ❑ Enable port access control

The AT-S39 management software comes pre-installed on the switch with default settings for all operating parameters. If the default settings are adequate for your network, you can use the switch as an unmanaged switch simply by connecting the unit to your network, as explained in the hardware installation guide, and powering ON the device.

Note
The default settings for the management software can be found in **Appendix A, AT-S39 Default Settings** on page 312.

To actively manage a switch, such as to change or adjust the operating parameters, you must access the switch's AT-S39 management software. The AT-S39 software has a menu interface that makes it very easy to use, and a special interface for managing a switch with a web browser.

There are four different ways to access the management software on an AT-8000 Series switch. In this guide, these methods are referred to as management sessions. They are:

- ❑ Local Management Session
- ❑ Telnet Management Session
- ❑ Web Browser Management Session
- ❑ SNMP Management Session

The following sections in this chapter briefly describe each type of management session.

Local Management Session

You can establish a local management session with an AT-8000 Series switch by connecting a terminal or a PC with a terminal emulator program to the RS232 Terminal port on the front panel of the switch, using a straight-through RS-232 cable. This type of management session is referred to as "local" because you must be physically close to the switch, such as in the wiring closet where the switch is located.

Once the session is started, a menu is displayed and you can make selections to configure and monitor the switch. You can configure all of a switch's operating parameters from a local management session.

Note
For instructions on starting a local management session, refer to **Starting a Local Management Session** on page 30.

Telnet Management Session

Any management workstation on your network that has the Telnet application protocol can be used to manage an AT-8000 Series switch. This type of management session is referred to in this guide as a remote management session because you do not have to be in the wiring closet where the switch you want to manage is located. You can manage the switch from any workstation on the network that has the application protocol.

To establish a Telnet management session with a switch, there must be at least one AT-8000 Series switch on the subnet that has been assigned an Internet Protocol (IP) address. Only one switch in a subnet needs to have an IP address. Once you have established a Telnet management session with the switch that has an IP address, you can use the enhanced stacking feature of the AT-S39 software to access all other AT-8000 Series switches in the same subnet.

Note
For further information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

Note
For instructions on how to start a Telnet management session, refer to **Starting a Telnet Management Session** on page 34.

A Telnet management session gives you complete access to all of a switch's operating parameters. You can perform nearly all the same functions from a Telnet management session as you can from a local management session.

Web Browser Management Session

You can also use a web browser to manage a switch. This too is referred to as remote management, just like a Telnet management session. You can manage a switch from any workstation on your network that has a web browser.

Note
For instructions on starting this type of management session, refer to **Starting a Web Browser Management Session** on page 227.

SNMP Management Session

Another way to remotely manage the switch is with an SNMP management program. A familiarity with Management Information Base (MIB) objects is necessary for this type of management.

The AT-S39 software supports the following MIBs:

- SNMP MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Interface Group MIB (RFC 1573)
- Ethernet MIB (RFC 1643)
- Remote Network MIB (RFC 1757)
- Allied Telesyn managed switch MIB

You must download the Allied Telesyn managed switch MIB (atistackinfo.mib and atiswitch.mib) file from the Allied Telesyn web site and compile the file with your SNMP program. For instructions, refer to your SNMP management documentation.

Note
SNMP management does not utilize the enhanced stacking feature. Consequently, you must assign an IP address to each switch to be managed with an SNMP program.

Management Access Levels

There are two levels of management access on an AT-8000 Series switch: Manager and Operator. When you log in as a Manager, you can view and configure all of a switch's operating parameters. When you log in as an Operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator by entering the appropriate password when you start an AT-S39 management session. To log in as a manager, type "manager" as the login and "friend" as the password. The default user name for operator is "operator" and the password is also "operator". Both login and password are case-sensitive.

Section II

Local and Telnet Management

The chapters in this section explain how to manage an AT-8000 Series switch from a local or Telnet management session. The chapters include:

- **Chapter 2**: **Starting a Local or Telnet Management Session** on page 28
- **Chapter 3**: **Basic Switch Parameters** on page 36
- **Chapter 4: Enhanced Stacking** on page 57
- **Chapter 5**: **Port Parameters** on page 65
- **Chapter 6**: **Port Security** on page 75
- **Chapter 7**: **Port Trunking** on page 82
- **Chapter 8**: **Port Mirroring** on page 92
- **Chapter 9**: **STP and RSTP** on page 96
- **Chapter 10**: **Virtual LANs Overview** on page 115
- **Chapter 11**: **Configuring User-Created VLANs** on page 137
- **Chapter 12**: **Multiple VLAN Configuration** on page 156
- **Chapter 13**: **MAC Address Table** on page 161
- **Chapter 14**: **Class of Service** on page 174
- **Chapter 15: IGMP Snooping** on page 177
- **Chapter 16**: **Broadcast Storm Control** on page 185
- **Chapter 17**: **TACACS+ and RADIUS Protocols** on page 191
- **Chapter 18**: **802.1x Port-Based Network Access Control** on

page 200

- **Chapter 19**: **Ethernet Statistics** on page 208
- **Chapter 20**: **File Downloads and Uploads** on page 213

Chapter 2
Starting a Local or Telnet Management Session

This chapter contains the procedure for starting a local or Telnet management session on an AT-8000 Series switch. The sections in the chapter are:

- **Local Management Session** on page 29
- **Telnet Management Session** on page 34

Local Management Session

On the front panel of the switch is a port labelled RS232 Terminal Port. You use this port to establish a local management session with the switch's AT-S39 management software.

A local management session is so named because you must be close to the switch, usually within a few meters, to start this type of management session. This typically means that you must be in the wiring closet where the switch is located.

A switch does not need an IP address to be managed from a local management session. You can start a local management session at any time on any AT-8000 Series switch in your network. Running a local management session does not interfere with the flow of Ethernet traffic through the unit.

Starting a local management session on a switch that has been configured as a Master switch of an enhanced stack allows you to manage all the switches in the subnet from the same local management session. You do not have to start a separate local management session for each switch. This can simplify network management.

Starting a local management session on a switch that is not part of an enhanced stack or that is a slave switch in an enhanced stack allows you to manage just that switch.

Note
For information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

Starting a Local Management Session

To start a local management session, perform the following procedure:

1. Connect one end of a straight-through RS232 cable with a DB-9 connector to the RS232 Terminal Port on the switch.

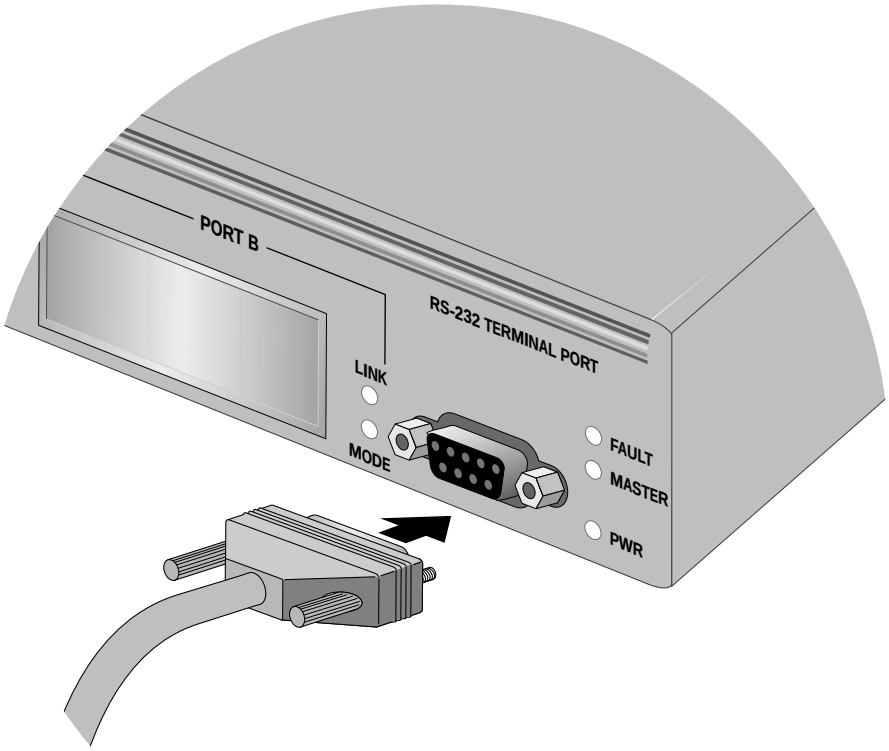

Figure 1 Connecting a Terminal or PC to the RS232 Terminal Port

2. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
   - ❑ Baud rate: 1200 bps to 115200 bps (default 9600; see Note below)
   - ❑ Data bits: 8
   - ❑ Parity: None
   - ❑ Stop bits: 1
   - ❑ Flow control: None

Note
The switch has an auto-detect feature on the serial port that auomatically determines the speed of the local terminal. Activate this feature by pressing the Return or Enter key twice on your keyboard when you initially start the local interface or within five seconds after powering on or resetting the switch. The switch responds by determining the speed of the terminal and automatically configuring the speed of the RS232 Terminal Port accordingly. Otherwise, the switch uses a default baud rate of 9600 bits per second (bps). The switch maintains the terminal port speed until the system is again powered on or reset. The range of the port's baud rate is 1200 to 115200 bps.

Note
The port settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

Note
During boot up, the switch displays the following prompt: `Press any key to stop image loading and go to Boot Prompt`. This message is intended for manufacturing purposes only. (If you inadvertently display the boot prompt (=>), type **boot** and press Return to start the switch.)

4. Press the Return key twice.

   If prompted for a password, enter the password for the management software. The default password for manager access is "friend". The default password for operator access is "operator". Logins and passwords are case-sensitive. For information on the two access levels, refer to **Management Access Levels** on page 25. (For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 48.)

The Main Menu is displayed.

```
Allied Telesyn Ethernet Switch AT-8024GB
Login Privilege: Manager
                    Main Menu

1 - Port Menu
2 - VLAN Menu
3 - Spanning Tree Menu
4 - Administration Menu
5 - System Config Menu
6 - MAC Address Tables
7 - Ethernet Statistics
8 - Diagnostics
9 - Enhanced Stacking
C - Command Line Interface


Q - Quit
```

Figure 2 Main Menu

To select a menu item, type the corresponding letter or number.

Pressing the Esc key or typing the letter **R** in a submenu or menu, returns you to the previous menu.

Please note the following:

- The Command Line Interface selection in the Main Menu is not described in this manual. For instructions on this option, refer to the **AT-S39 Command Line Interface User's Guide**.
- If a dollar sign ($) is displayed instead of the Main Menu, the console interface has been configured for a command line interface management session. To display the Main Menu, type **menu** and press Return.
- During boot up, the switch displays the following message: `Press any key to stop image loading and go to Boot Prompt`. This message is for manufacturing purposes only. If you do inadvertently display the boot prompt (=>), type **boot** and press Return to start the switch's software.

Enhanced Stacking

When you start a local management session on a switch that has been designated as the Master switch of an enhanced stack, you can manage all the switches in the same subnet from the same management session. This can save you the time and trouble of having to start a separate local management session each time you want to manage a switch in your network. It can also save you from having to go to the different wiring closets where the switches are located.

For information on enhanced stacking and how to manage different switches from the same management session, refer to **Chapter 4, Enhanced Stacking** on page 57.

Quitting from a Local Session

To quit a local session, return to the Main Menu and type **Q** for Quit.

You should always exit from a management session when you are finished managing a switch. This can prevent unauthorized individuals from making changes to a switch's configuration should you leave your management station unattended.

Note
You cannot operate both a local management session and a Telnet management session on the same switch simultaneously. Failure to properly exit from a local or Telnet management session may block future management sessions.

Telnet Management Session

You can use the Telnet application protocol from a workstation on your network to manage an AT-8000 Series switch. This type of management is referred to as remote management because you do not have to be physically close to the switch to start the session, such as with a local management session. Any workstation on your network that has the application protocol can be used to manage the switch.

In terms of functionally, there are almost no differences between managing a switch locally through the RS232 Terminal Port and remotely with the Telnet application protocol. You see the same menu selections and have nearly the same management capabilities.

Starting a Telnet management session requires that there be at least one AT-8000 Series switch on your network that has an IP address. The switch with the IP address is referred to as the master switch. Once you have started a Telnet management session on the master switch, you will have management access to all the other AT-8000 Series switches that reside in the same subnet.

Note

Note
For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

Starting a Telnet Management Session

To start a Telnet management session, specify the IP address of the master switch of the enhanced stack in the Telnet application protocol and enter the management software password when prompted. The default password for manager access is “friend”. The default password for operator access is “operator”. Logins and passwords are case-sensitive. For information on the two access levels, refer to **Management Access Levels** on page 25. (For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 48.)

The Main Menu of a Telnet management session is the same menu that you see in a local management session, shown in Figure 2 on page 32. Nearly all the functions from a local management session are available to you from a Telnet management session.

The menus also function the same. To make a selection, type its corresponding number of letter. To return to a previous menu, type **R** or press ESC twice.

Note
You can run only one Telnet management session on a switch at a time. Additionally, you cannot run both a Telnet management session and a local management session on the same switch at the same time.

Quitting from a Telnet Management Session

To end a Telnet management session, return to the Main Menu and type **Q** for Quit.

Chapter 3
Basic Switch Parameters

This chapter contains a variety of information and procedures. There is a discussion on when to assign an IP address to a switch and the different ways that you can go about it. There are also procedures for resetting the switch, activating the original switch default settings, and more.

Sections in the chapter include:

- ❑ **When Does a Switch Need an IP Address?** on page 37
- ❑ **Configuring an IP Address and Switch Name** on page 39
- ❑ **Activating the BOOTP and DHCP Services** on page 42
- ❑ **Configuring SNMP Community Strings and Trap IP Addresses** on page 44
- ❑ **Resetting a Switch** on page 47
- ❑ **Configuring the AT-S39 Software Security Features** on page 48
- ❑ **Viewing the AT-S39 Version Number and Switch MAC Address** on page 52
- ❑ **Pinging a Remote System** on page 53
- ❑ **Returning the AT-S39 Software to the Factory Default Values** on page 54
- ❑ **Configuring the Console Startup Mode** on page 55
- ❑ **Configuring BALUN Cable Detection** on page 56

When Does a Switch Need an IP Address?

One of the tasks to building or expanding a network is deciding which of the managed switches need to be assigned unique IP addresses. The rule used to be that a managed switch needed an IP address if you wanted to manage it remotely, such as with the Telnet application protocol. However, if a network contained a lot of managed switches, having to assign each one an IP address was often cumbersome and time consuming. It was also often difficult keeping track of all the IP addresses.

The enhanced stacking feature of the AT-8000 Series switch simplifies all this. With enhanced stacking, you need assign an IP address to only one AT-8000 Series switch in each subnet in your network. The switch with the IP address is referred to as the Master switch of the subnetwork. All switches in the same subnet share the IP address.

Starting a local or remote management session on the Master switch automatically gives you complete management access to all the other switches in the same subnet.

This feature has two primary benefits. First, it helps reduce the number of IP addresses you have to assign to your network devices. Second, it allows you to configure multiple switches through the same local or remote management session.

If your network consists of multiple subnets, you must assign a unique IP address to at least one switch in each subnet. The switch with the IP address will be the Master switch of that subnet.

When you assign a switch an IP address, you must also assign it a subnet mask. The switch uses the subnet mask to determine which portion of an IP address represents the network address and which the node address.

You must also assign the switch a gateway address if there is a router between the switch and the remote management workstation. This gateway address is the IP address of the router through which the switch and management station will communicate.

Note
For further information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

If you do not plan to remotely manage any of the AT-8000 Series switches in your network, then you do not need to assign any of them an IP address. The switches will operate fine without an IP address and you will still be able to manage them completely using local management sessions.

How Do You Assign an IP Address?

Once you have decided which, if any, switches on your network need an IP address, you have to access the AT-S39 software on the switches and assign the addresses. There are actually two ways in which a switch can obtain an IP address.

The first method is for you to assign the IP configuration information manually. The procedure for this is explained in **Configuring an IP Address and Switch Name** on page 39. Initially assigning an IP address to a switch can only be done through a local management session.

The second method is for you to activate the BOOTP and DHCP services on the switch and have the switch automatically download its IP configuration information from a BOOTP or DHCP server on your network. This procedure is explained in **Activating the BOOTP and DHCP Services** on page 42.

Configuring an IP Address and Switch Name

The procedure in this section explains how to manually assign an IP address, subnet mask, and gateway address to the switch from a local or Telnet management session. (If you want the switch to obtain its IP configuration from a DHCP or BOOTP server on your network, go to the procedure **Activating the BOOTP and DHCP Services** on page 42.)

This procedure also explains how to assign a name to the switch, along with other optional information, such as the name of the administrator responsible for maintaining the unit and the location of the switch.

To manually set a switch's IP address, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.

   The Administration Menu in Figure 3 is displayed.

```
      Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
               Administration Menu

1 - IP Address ........ 0.0.0.0
2 - Subnet Mask ....... 0.0.0.0
3 - Default Gateway ... 0.0.0.0
4 - System Name .......
5 - Administrator .....
6 - Comments ..........
7 - Set Password ......
8 - BOOTP/DHCP ........ Disabled

9 - Reset Switch
A - Server-based Authentication
D - Downloads & Uploads
P - Ping a Remote System

R - Return to Previous Menu

Enter your selection?
```

Figure 3 Administration Menu

2. Change the parameters as desired.

   The parameters in the IP Parameters menu are described below:

   1 - IP Address
   This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program, or if you want a switch to function as the Master switch of an enhanced stack.

   2 - Subnet Mask
   This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch.

   3 - Default Gateway
   This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router.

   4 - System Name
   This parameter specifies a name for the switch (for example, Sales Ethernet switch). This parameter is optional.

   Note
   It is advisable that you assign each switch a name. The names can help you identify the various switches when you manage them and avoid performing a configuration procedure on the wrong switch.

   5 - Administrator
   This parameter specifies the name of the network administrator responsible for managing the switch. This parameter is optional.

   6 - Comments
   This parameter specifies additional information about the Fast Ethernet switch, such as its location (for example, 4th Floor - wiring closet 402B). This parameter is optional.

   7 - Set Password
   This parameter is used to change the Manager and Operator's login passwords. For instructions, refer to **Configuring the Management Passwords** on page 48.

   8 - BOOTP/DHCP
   This selection activates and deactivates the BOOTP and DHCP services on the switch. For information on this selection, refer to **Activating the BOOTP and DHCP Services** on page 42.

9 - Reset Switch
This selection resets the switch.

A - Server-based Authentication
This selection is used to configure the TACACS+ and RADIUS authentication protocols on the switch. For information on this feature, refer to **Chapter 17, TACACS+ and RADIUS Protocols** on page 191.

Downloads and Uploads
For information on this selection, refer to **Chapter 20**, **File Downloads and Uploads** on page 213.

R - Ping a Remote System
For information on this selection, refer to **Pinging a Remote System** on page 53.

3. After you have set the parameters, type **S** to select Save Configuration Changes.

Note
A change to any of the parameters in this menu, including the IP address, subnet mask, or gateway address, are immediately activated on a switch.

Activating the BOOTP and DHCP Services

The BOOTP and DHCP application protocols were developed to simplify network management. They are used to automatically assign IP configuration information to the devices on your network, such as an IP address, subnet mask, and a default gateway address.

An AT-8000 Series switch supports these protocols and can obtain its IP configuration information from a BOOTP or DHCP server on your network. If you activate this feature, the switch will seek its IP address and other IP configuration information from a BOOTP or DHCP server on your network whenever you reset or power ON the device.

Naturally, for this to work there must be a BOOTP or DHCP server residing on your network and you must configure the service by entering in the switch's MAC address.

BOOTP and DHCP services typically allow you to specify how the IP address is to be assigned to the switch. Choices are static and dynamic. If you choose static, the server will always assign the same IP address to the switch when the switch is reset or powered ON. This is the preferred configuration. Since the BOOTP and DHCP services always assigns the same IP address to a switch, you will always know which IP address to use when you need to remotely manage a particular switch.

If you choose dynamic, the server will assign any unused IP address that it has not already assigned to another device. This means that a switch might have a different IP address each time you reset or power cycle the device, making it difficult for you to remotely manage the unit.

Note
The BOOTP and DHCP option is disabled by default on the switch.

To activate or deactivate the BOOTP and DHCP protocols on the switch, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.

   The Administration in Figure 3 on page 39 is displayed.

2. Type **8** to select BOOTP/DHCP.

   The following prompt is displayed:

   ```
   BOOTP/DHCP (E-Enabled, D-Disabled):
   ```

3. Type **E** to enable BOOTP and DHCP services on the switch or **D** to disable the services and press Return. The default is disabled.

4. Type **S** to select Save Configuration Changes.

Note

If you activated BOOTP/DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response.

Configuring SNMP Community Strings and Trap IP Addresses

To configure the SNMP community strings for the switch and to assign up to four IP addresses of management stations to receive traps from the switch, perform the following procedure:

> **Note**
> SNMP access is disabled by default. To enable SNMP access, refer to **Configuring Management Access** on page 51.

1. From the Main Menu, type **5** to select System Config Menu.

   The System Configuration Menu in Figure 4 is displayed.

```
Allied Telesyn AT-8024 Ethernet Switch
Login Privilege: Manager
                 System Config Menu


1 - MAC Aging Time ..................... 300 seconds
2 - Switch Mode ........................ Tagged
3 - Console Disconnect Timer Interval . 10 minute(s)
4 - Web Server Status .................. Enabled
5 - SNMP Access ........................ Disabled
6 - Console Startup Mode ............... Menu
7 - BALUN Cable Detection .............. Disabled
8 - Reset to Factory Defaults

A - Advanced Configuration

R - Return to Previous Menu

Enter your selection?
```

Figure 4 System Configuration Menu

2. From the System Configuration Menu, type **A** to select Advanced Configuration.

   The Advanced Configuration menu in Figure 5 is displayed.

```
     Allied Telesyn AT-8024 Ethernet Switch
Login Privilege: Manager
          Advanced Configuration Menu


1 - IGMP Snooping Configuration
2 - Broadcast Timers Setup
3 - SNMP Configuration

R - Return to Previous Menu

Enter your selection:
```

Figure 5 Advanced Configuration Menu

3. From the Advanced Configuration menu, type **3** to select SNMP Configuration. The SNMP Configuration menu in Figure 6 is displayed.

```
     Allied Telesyn AT-8024 Ethernet Switch
Login Privilege: Manager
              SNMP Configuration


1 - GET Community ..............  public
2 - SET Community ..............  private
3 - Trap Community .............  public

4 - Trap Receiver 1 ............  0.0.0.0
5 - Trap Receiver 2 ............  0.0.0.0
6 - Trap Receiver 3 ............  0.0.0.0
7 - Trap Receiver 4 ............  0.0.0.0

S - Save Configuration Changes
R - Return to Previous Menu


Enter your selection:
```

Figure 6 SNMP Configuration Menu

4. Adjust the parameters as desired. To change a value, type its corresponding number and, when prompted, enter the new value. The parameters are described below.

   1 - GET Community
   2 - SET Community
   3- Trap Community
   Use these parameters to set a switch's SNMP community strings.

   4 - Trap Receiver 1
   5 - Trap Receiver 2
   6 - Trap Receiver 3
   7 - Trap Receiver 4
   Use these selections to specify the IP addresses of up to four management workstations on your network to receive traps from the switch.

5. After making your changes, type **S** to select Save Configuration Changes.

   Changes to the SNMP parameters are immediately activated on the switch.

Resetting a Switch

To reset a switch, perform the following procedure:

1. From the Main Menu, type **4** to select Administrator Menu.
2. From the Administrator Menu, type **9** to select Reset Switch.

   The following prompt is displayed:

   ```
   Do you want to proceed with the switch reboot?
   [Yes/No] ->
   ```

3. Type **Y** to reset the switch or **N** to cancel this procedure.

   The following prompt is displayed:

   ```
   Please press <ENTER> key TWICE to proceed with the
   Switch Reset...
   ```

4. Press the Return key twice.

   The switch reloads its operating system, a task requiring approximately 20 seconds to complete.

Caution
The switch will not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Configuring the AT-S39 Software Security Features

The AT-S39 software has several security features that can help prevent unauthorized individuals from changing the parameter settings of an AT-8000 Series switch. The security features are:

- Manager and Operator Passwords - The management software has two standard, management login accounts: Manager and Operator. The Manager acount allows you to configure all switch parameters, while the Operator account only allows you to view the parameter settings. The default login for Manager access is "manager" and the password is "friend". Both login and password for Operator access are "operator". Logins and passwords are case-sensitive. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 48. (You can create additional management login accounts for the switch if your network contains a TACACS+ or RADIUS authentication protocol server. For instructions, refer to **Chapter 17, TACACS+ and RADIUS Protocols** on page 191.)
- Console Timeout - This parameter causes the management software to automatically end a management session if it does not detect any activity from the local or remote management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. The default for the console timeout value is 10 minutes. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 51.
- Web Access - You can disable the web browser management feature on the switch, and so prevent individuals from managing the switch remotely using a web browser. By default, Web access is enabled. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 51.
- SNMP Access - You can also disable the SNMP management feature on the switch, and so prevent individuals from managing the switch remotely using a SNMP management program. By default, SNMP access is disabled. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 51.

Configuring the Management Passwords

There are two levels of management access on an AT-8000 Series switch: Manager and Operator. When you log in as a Manager, you can view and configure all of a switch's operating parameters. When you log in as an Operator, you can only view the operating parameters; you cannot change any values.

You log in as a Manager or an Operator by entering the appropriate password when you start an AT-S39 management session. The default password for Manager access is "friend". The default password for Operator access is "operator". Logins and passwords are case-sensitive.

To change the Manager or Operator password, perform the following procedure:

1. From the Main Menu, type **4** to select Administrator Menu.
2. From the Administrator Menu, type **7** to select Set Password. The Passwords Menu in Figure 7 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                  Passwords Menu


1 - Set Manager Password
2 - Set Operator Password

R - Return to Previous Menu

Enter your selection?
```

Figure 7 Passwords Menu

3. Type **1** to change the Manager password or type **2** to change the Operator password.
4. When prompted, enter the current Manager or Operator password.
5. When prompted, enter the new Manager or Operator password.
6. When prompted, re-enter the new Manager or Operator password.

Note
The password can be from 0 to 20 alphanumeric characters. Logins and passwords are case-sensitive.

Note
The two passwords should be different. If both passwords are the same, the management software will always assume that you wish to log in as Manager.

Caution

You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

Configuring Management Access

To configure the console timer, web access, SNMP access, and TFTP server security features of the AT-S39 management software, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.

   The System Configuration Menu Figure 4 on page 44 is displayed.

2. To configure the console timer, type **3** to select Console Disconnect Timer Interval and, when prompted, enter a value of from 1 to 60 minutes. The default value is ten minutes.

   For example, if you specify 2 minutes, the AT-S39 management software automatically ends a management session if it does not detect any activity from the local or remote management station after 2 minutes.

3. To configure web browser access, type **4** to select Web Server Access and, when prompted, type **E** to enable web access or **D** to disable web access. The default value is enabled.

   For example, if you disable web access, no one will be able to manage the switch remotely using a web browser.

4. To configure SNMP access, type **5** to select SNMP Access and, when prompted, type **E** to enable SNMP management access or **D** to disable it. The default value is disabled.

   For example, if you disable SNMP access, no one will be able to manage the switch remotely using an SNMP management program.

5. After you have made the desired changes, type **S** to select Save Configuration Changes.

   Your changes are immediately activated on the switch.

Viewing the AT-S39 Version Number and Switch MAC Address

The procedure in this section displays the following switch information:

- ❑ AT-S39 version number
- ❑ Bootloader version number
- ❑ Serial number
- ❑ MAC Address

To display the information, type **8** to select Diagnostics from the Main Menu. The Diagnostics menu in Figure 8 is displayed.

```
Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                              Diagnostics

1 - Application Software Version .... AT-S39 v3.1.0
2 - Application Software Build Date . Mar 14 2003 19:32:40
3 - Bootloader Version ............... ATS39_LOADER v2.0.1
4 - Bootloader Build Date ........... Jul 29 2002 16:37:14
5 - Serial Number ................... S05248014600028
6 - MAC Address ..................... 00:30:84:52:03:80
7 - Uplink Information

R - Return to Previous Menu

Enter your selection?
```

Figure 8 Diagnostics Menu

The information displayed in selections 1 through 6 in this menu cannot be changed. For information on option 7, refer to **Displaying Uplink Information** on page 73.

Pinging a Remote System

You can instruct the switch to ping a remote device on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.
2. From the Administration Menu, type **P** to select Ping a Remote System.

   The following prompt is displayed:

   ```
   Please enter an IP address ->
   ```

3. Enter the IP address of the end node you want the switch to ping and press Return.

   The results of the ping command are displayed on the screen. To stop the ping, press any key.

Returning the AT-S39 Software to the Factory Default Values

The procedure in this section returns all AT-S39 software parameters to their default values. This procedure also deletes any VLANs that you have created on the switch.

> **Note**
> The AT-S39 software default values can be found in **Appendix A, AT-S39 Default Settings** on page 312.

To return the AT-S39 management software to its default settings, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **8** to select Reset to Factory Defaults.

   The following prompt is displayed:

   ```
   Are you sure you want to reset to Factory Defaults?
   [Yes/No] ->
   ```

3. Type **Y** for yes or **N** for no.

   The following prompt is displayed:

   ```
   Do you want to reset IP, Subnet and Gateway as well?
   [Yes/No] ->
   ```

4. If you type **Y** for yes, all switch parameters including the IP address, subnet mask, and gateway address are changed to their default values. If you type **N** for no, all switch parameters excluding the IP address, subnet mask, and gateway address are changed to their default values.

   The following prompt is displayed:

   ```
   The Factory Defaults take effect only after the
   Switch reboots.

   Do you want to Reboot the Switch now? [Yes/No] ->
   ```

5. Type **Y** to reset the switch.

   The operating parameters are returned to their default values and the switch is reset.

> **⚠ Caution**
> The switch will not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Configuring the Console Startup Mode

You can configure the AT-S39 software to display either the Main Menu or the command line interface prompt ($) whenever you start a local management session. The default is the Main Menu.

To change the console startup mode, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **6** to select Console Startup Mode.

   The following prompt is displayed:

   ```
   Enter Console Mode (M-Menu, C-CLI):
   ```

3. Type **M** if you want a local management session to always start with the Main Menu, or **C** if you want it to display the command line interface prompt.

   A change to the console startup mode takes effect the next time you start a local management session.

Configuring BALUN Cable Detection

You can configure the AT-S39 software to detect loopback cables for all 10/100/1000 copper ports. When a loopback cable is detected, the port is set to MANUAL/10/HDX/MDIX and a message is displayed on the console. When the loopback cable is replaced with a good cable, the original port settings are restored.

To configure the switch to enable or disable balun cable detection, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **7** to select BALUN Cable Detection. The following prompt is displayed:

   ```
   Enter BALUN Cable Detection Status (E-Enabled, D-Disabled) :
   ```

3. Select **E** to enable cable detection or select **D** to disable cable detection.

Chapter 4
Enhanced Stacking

This chapter explains the enhanced stacking feature. The sections in this chapter include:

- ❑ **Enhanced Stacking Overview** on page 58
- ❑ **Setting a Switch's Enhanced Stacking Status** on page 61
- ❑ **Selecting a Switch in an Enhanced Stack** on page 63

Note
When managing the remote/telnet interface do not reset the IP address to null. This will cause disconnection without local management intervention.

Enhanced Stacking Overview

The enhanced stacking feature can make it easier for you to manage the AT-8000 Series switches in your network. It offers the following benefits:

- ❑ You can manage up to 24 switches from one local or remote management session. This eliminates the need of having to initiate a separate management session for each switch in your network.
- ❑ The switches can share the same IP address. This reduces the number of IP addresses that you need to assign to your network devices for remote management.
- ❑ Remotely managing a new switch in your network is simplified. You simply connect it to your network. Once connected to the network, you can begin to manage it immediately from any workstation in your network.

Guidelines

There are a few guidelines to keep in mind when implementing enhanced stacking for your network:

- ❑ Each subnet in your network can only have one enhanced stack. You cannot have multiple enhanced stacks in a subnet.
- ❑ Each subnet must have at least one master switch.
- ❑ You must assign the master switch an IP address and subnet mask.
- ❑ You must change the master switch's stacking status to Master.

There are three basic steps to implementing this feature on your network:

1. You must select a switch in your network to function as the master switch of the stack.

   You can select any AT-8000 Series switch to act as the master switch of an enhanced stack. For networks that consist of more than one subnet, there must be at least one master switch in each subnet.

   It is recommended that each subnet have two master switches. That way, should you remove one of the master switches from the network, such as for maintenance, you all still be able to remotely manage the switches in the subnet using the other master switch.

2. You must assign the master switch an IP address and subnet mask.

   A master switch must have an IP address and subnet mask. The other switches in an enhanced stack, referred to as slave switches, do not.

   If an enhanced stack will have more than one master switch, you must assign each master switch a unique IP address.

   Note
   You can set the IP address manually or activate the BOOTP and DHCP services on a master switch and have the master switch obtain its IP information from a BOOTP or DHCP server on your network. Initially assigning an IP address or activating the BOOTP and DHCP services can only be performed through a local management session.

   For instructions on how to set the IP address manually, refer to **Configuring an IP Address and Switch Name** on page 39. For instructions on activating the BOOTP and DHCP services, refer to **Activating the BOOTP and DHCP Services** on page 42.

3. Change the enhanced stacking status of the master switch to Master.

   This is explained in the procedure **Setting a Switch's Enhanced Stacking Status** on page 61.

   Note
   By default, the switches are sorted in the menu by MAC address. You can sort the switches by name as well. This is accomplished by selecting **S** for Sort Switches in New Order.

Figure 9 is an example of the enhanced stacking feature.

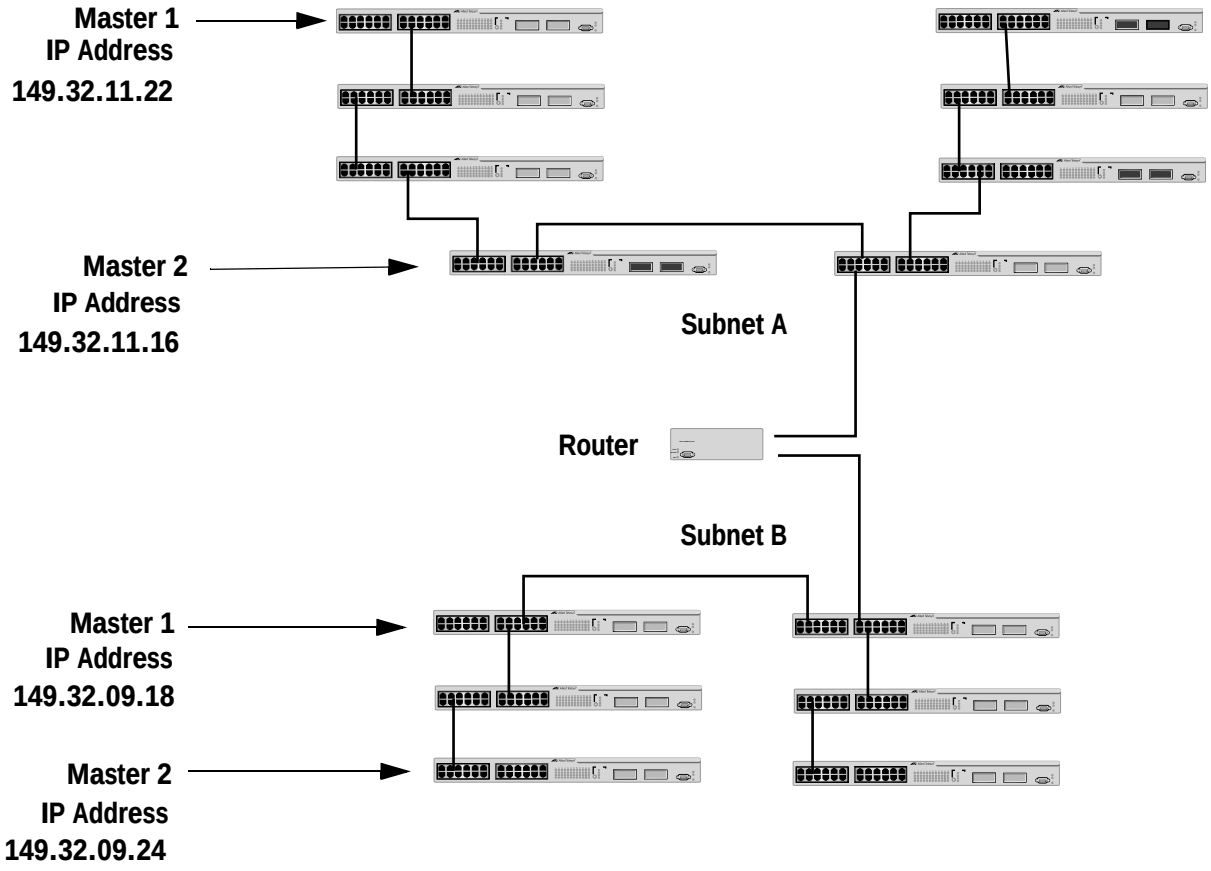

Figure 9 Enhanced Stacking Example

The example consists of a network of two subnets interconnected with a router. Two switches in each subnet have been selected as the master switches of their respective subnets, and each has been assigned a unique IP address.

To manage the switches of a subnet, you could start a local management session or a remote Telnet management session with one of the master switches in the subnet. You would then have management access to all the AT-8000 Series switches in the same subnet.

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master switch, slave switch, or unavailable. Each status is described below:

- Master switch - A master switch of a stack can be used to manage all the other AT-8000 Series switches in a subnet. Once you establish a local or remote management session with the Master switch, you can access and manage all the switches in the subnet.

  A master switch must have a unique IP address. You can manually assign a master switch an IP address or activate the BOOTP and DHCP services on the switch.

- Slave switch - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask.

- Unavailable - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally. To be managed remotely, a switch with an unavailable stacking status must be assigned a unique IP address.

Note
The default setting for a switch is Slave.

To adjust a switch's enhanced stacking status, perform the following procedure:

1. From the Main Menu, type **9** to select Enhanced Stacking.

   The Enhanced Stacking menu in Figure 10 is displayed.

```
          Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                    Enhanced Stacking


1 - Switch State-(M)aster/(S)lave/(U)navailable.... Master
2 - Stacking Services

S - Save Configuration Changes
R - Return to Previous Menu
Enter your selection?
```

Figure 10 Enhanced Stacking Menu

The menu displays the current status of the switch at the end of selection “1 - Switch State.” For example, the switch’s current status in the figure above is Master.

Note
The “2 - Stacking Services” selection in the menu is available only on master switches.

2. To change a switch’s stacking status, type **1** to select Switch State.

   The following prompt is displayed.

   ```
   Enter new setup (M/S/U) ->
   ```

3. Type **M** to change the switch to a master switch, **S** to make it a slave switch, or **U** to make the switch unavailable. Press Return.

4. Type **S** to select Save Configuration Changes.

   A change to the status is immediately activated on the switch.

Selecting a Switch in an Enhanced Stack

The first thing that you should do before performing any procedure on a switch in an enhanced stack is check to be sure that you are performing it on the correct switch. If you assigned system names to your switches, this should be easy. The name of the switch being managed is always displayed at the top of every management menu.

When you start a management session on the Master switch of a subnet, you are by default addressing that particular switch. The management tasks that you perform effect only the master switch.

To manage a slave switch or another Master switch in the subnet, you need to select it from the management software.

To select a switch to manage in an enhanced stack, perform the following procedure:

1. From the Main Menu, type **9** to select Enhanced Stacking.
2. From the Enhanced Stacking menu, type **2** to select Stacking Services.

   The menu in Figure 11 is displayed.

```
          Allied Telesyn Ethernet Switch AT-8024GB
                        Sales Switch

Login Privilege: Manager

                      Stacking Services

                              Switch     Software     Switch
Num  MAC Address    Name       Mode       Version      Model
-------------------------------------------------------------


G - Get/Refresh List of Switches
S - Sort Switches in New Order
A - Access Switch
I - Image Download to Remote Switches
C - Config Download to Remote Switches
B - Boot Loader Download to Remote Switches
R - Return to Previous Menu

Enter your selection?
```

Figure 11 Stacking Services Menu

3. Type **G** to select Get/Refresh List of Switches.

   The Master switch polls the network for all slave and Master switches in the subnet and displays a list of the switches in the Stacking Services menu.

   Note
   The Master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of Unavailable.

   Note
   The selections I, C, and B for downloading image and bootloader files are explained in **Chapter 20**, **File Downloads and Uploads** on page 213.

   By default, the switches are sorted in the menu by MAC address. You can sort the switches by name as well. This is accomplished with the selection S - Sort Switches in New Order.

4. To manage a different switch in an enhanced stack, type **A** to select Access Switch.

   A prompt similar to the following is displayed:

   ```
   Enter the switch number -> [1 to 24}
   ```

5. Type the number of the switch in the list you want to manage.

   A prompt is displayed if the switch has been assigned a password.

6. Enter the switch's password and press Return.

   The default password for manager access is "friend". The default password for operator access is "operator". Logins and passwords are case-sensitive.

   The Main Menu of the selected switch is displayed. You now can manage the switch. Any management tasks you perform effect only the selected switch.

Returning to the Master Switch

When you have finished managing a slave switch and want to manage another switch in the subnet, return to the Main Menu of the slave switch and type **Q** for Quit. This returns you to the Stacking Services menu. Once you see that menu, you are again addressing the Master switch from which you started the management session.

You can either select another switch in the list to manage or, if you want to manage the Master switch, return to the master switch's Main Menu by typing **R** twice.

Chapter 5
Port Parameters

The chapter contains procedures for viewing and changing the parameter settings for the individual ports on a switch.

This chapter contains the following procedures:

- **Displaying Port Status** on page 66
- **Configuring Port Parameters** on page 69
- **Displaying Uplink Information** on page 73

Displaying Port Status

To display the status of the ports on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.

   The Port Menu in Figure 12 is displayed.

```
      Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                    Port Menu


1 - Port Configuration
2 - Port Mirroring
3 - Port Trunking
4 - Port Status
5 - Port Security
6 - Port Access Control

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 12 Port Menu

2. From the Port Menu, type **4** to select Port Status.

The Port Status window is displayed (see Figure 13).

```
                Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                              Port Status


Prt  Link  Neg    MDIO Spd  Dplx  PVID   VlanID  Flow      State
-------------------------------------------------------------------------
001  Up    Auto   MDI  10   Half  00001  00001   Disabled  Forwarding
002  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
003  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
004  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
005  Up    Auto   MDI  10   Half  00001  00001   Disabled  Forwarding
006  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
007  Up    Auto   MDI  100  Full  00001  00001   Disabled  Forwarding
008  Up    Auto   MDI  10   Half  00001  00001   Disabled  Forwarding

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 13 Port Status Window

The information in this window is for viewing purposes only. The columns in the window are described below:

Prt

The port number.

Link

The status of the link between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Neg

The status of Auto-Negotiation on the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode.

Manual - Indicates that the operating speed and duplex mode have been set manually.

MDIO
The operating configuration of the port. Possible values are Auto, MDI, MDI-X. The status Auto indicates that the port is automatically determining the appropriate MDI or MDI-X setting.

Spd
The operating speed of the port. Possible values are:

10 - 10 Mbps

100 - 100 Mbps

1000 - 1000 Mbps (AT-8024GB switch only)

Dplx
The duplex mode of the port. Possible values are half-duplex and full-duplex.

PVID
The port VLAN identifier currently assigned to the port.

VlanID
The VLAN identifier of the VLAN in which the port is an untagged member. This column will not include the VIDs of the VLANs where the port is a tagged member.

Flow
The flow control setting for the port. Possible values are:

None - No flow control on the port.

Transmit - Flow control only as packets are being transmitted out the port.

Receive - Flow control only on as packets are being received on the port.

Both - Flow control for both packets entering and leaving the port.

State
The current operating status of the port. Possible values are:

Forwarding - The port is sending and receiving Ethernet frames.

Disabled - The port has been manually disabled.

Configuring Port Parameters

To configure the parameter settings for a port on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **1** to select Port Configuration.

   The following prompt is displayed:

   ```
   Enter Ports List ->
   ```

3. Enter the number of the port you want to configure and press Return. To configure a range of ports, enter the first port of the range.

   The following prompt is displayed:

   ```
   Ending Port to Configure [1 to 24] ->
   ```

4. To configure only one port, enter the same port number as you entered in Step 3 and press Return. To configure a range of ports, enter the last port number in the range. The Port Configuration menu in Figure 14 is displayed.

```
Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                  Port Configuration

Configuring Ports 4
0 - Status ............ Forwarding
1 - Negotiation ....... Auto
4 - Flow Control ...... None
5 - Advertise 10FDX ... Yes
6 - Advertise 10HDX ... Yes
7 - Advertise 100FDX .. Yes
8 - Advertise 100HDX .. Yes
M - MDI/MDIX Mode ..... Auto
B - Broadcast Control . No Broadcast Control

S - Save Configuration changes
F - Force Renegotiation
X - Reset Port
R - Return to Previous Menu

Enter your selection?
```

Figure 14 Port Configuration Menu

Note
The example Port Configuration menu in the figure above is for a 10/100 Mbps twisted pair port. The menu for a fiber optic port, a GBIC module, or a stacking module will contain a subset of the parameters.

5. Adjust the port parameters as desired. You adjust a parameter by typing its number. This toggles the parameter through its possible settings. The parameters are described below.

   0 - Status
   You use this selection to enable or disable a port. When disabled, a port will not receive or transmit frames.

   You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections.

   Possible settings are:

   Forwarding - The port will receive and forward packets. This is the default setting.

   Disabled - The port will not receive or forward packets.

   1 - Negotiation
   You use this selection to configure a port for Auto-Negotiation or to manually set a port's speed and duplex mode.

   If you select Auto for Auto-Negotiation, which is the default, the switch will set both speed and duplex mode for the port automatically.

   If you select Manual, two additional selections are displayed in the menu:

   ```
   2 - Speed ............. 0100
   3 - Duplex .............Full-Duplex
   ```

   You use these two selections to set the port's speed and duplex mode. The possible settings for the 2 - Speed selection are:

   0010 - 10 Mbps

   0100 - 100 Mbps

   1000 - 1000 Mbps (AT-8024GB switch only)

   The possible settings for 3 - Duplex are Full-duplex and Half-duplex.

Flow Control
Flow control applies only to ports operating in full-duplex mode. The switch uses a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time.

Possible settings are:

None - No flow control on the port.

Transmit - Flow control only as packets are being transmitted out the port.

Receive - Flow control only on as packets are being received on the port.

Both - Flow control for both packets entering and leaving the port.

5 - Advertise 10FDX
6 - Advertise 10HDX
7 - Advertise 100FDX
8 - Advertise 100HDX
These selections are used for ports configured for Auto-Negotiation. During Auto-Negotiation, a switch port determines the appropriate speed and duplex mode by advertising its capabilities to the end node connected to it.

By default, a switch port will advertise its full capabilities, which in the case of a port on an AT-8000 Series switch are 10 or 100 Mbps speed and half- or full-duplex mode.

You can use these four selections to limit the capabilities a switch port will advertise during Auto-Negotiation. For example, if you set the selection 8 - Advertise 100HDX to No, the switch port will not advertise that it is capable of 100 Mbps, half-duplex operation.

Note
In most network environments you should leave all Auto-Negotiation advertisements activated, which is the default setting.

M - MDI/MDIX Mode
Use this selection to set the wiring configuration of the port. If you set this to Auto, which is the default setting, the port will configure itself automatically according to the end node connected to it.

If desired, you can set the wiring configuration manually by selecting either MDI or MDIX.

Note
The Auto setting is not available if you set a port's speed and duplex mode manually.

B - Broadcast Control
For background information on this selection and instructions on how to set the option, refer to **Broadcast Storm Control Overview on page 186** and **Configuring the Maximum Broadcast Frame Count on page 190**.

6. Once you have set the port parameters, type **S** to select Save Configuration Changes.

   Configuration changes are immediately activated on a port.

The Port configuration menu features a Reset Port selection. You can use this option to reset the selected port. This can prove useful in situations where a port is experiencing a problem establishing a valid connection to the end node.

The menu also has a Force Renegotiation selection, which, when selected, prompts the port to Auto-Negotiate with the end node. This can be helpful if you believe that a port and end node are not operating at the same speed and duplex mode.

Displaying Uplink Information

The AT-S39 management software can display basic manufacturer information about a GBIC module in an AT-8024GB switch or the fiber optic ports in an AT-8026FC switch.

To display uplink information, perform the following procedure:

1. From the Main Menu, type **8** to select Diagnostics.
2. From the Diagnostics menu, type **7** to select Uplink Information.

   The GBIC Information menu in Figure 15 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
             Uplink Information Menu

1 - Uplink Information
R - Return to Previous Menu

Enter your selection?
```

Figure 15 Uplink Information Menu

3. Type **1** to select Uplink Information.

   The following prompt is displayed:

   ```
   Enter Uplink Port number -> [25 to 26]
   ```

4. Type either **25** or **26**; these are the port numbers for GBIC modules in an AT-8024GB switch. Press Return.

The management software displays a menu containing basic information about the GBIC module. Figure 16 is an example of the menu.

```
Allied Telesyn AT-8024GB Ethernet Switch
Login Privilege: Manager
                    Uplink Information Menu

Port Number ................... 25
Type of Serial Tranceiver ..... Unknown
Extended Serial Tranceiver .... Module Not Defined
Connector Type ................ Unknown
Elect/Opt Tranceiver ..........
Serial Encoding ............... Unspecified
Nominal bit rate(100Mbits/s) .. 0
Length 9/125 mm Fib. (k) ...... 0
Length 9/125 um Fib. (100m) ... 0
Length 50/125 um Fib. (10m) ... 0
Length 62.5/125 um Fib. (10m) . 0

N - Next Page
R - Return to Previous Menu

Enter your selection?
```

Figure 16 GBIC Information Menu

The information in the menu cannot be changed and is for viewing purposes only.

Chapter 6
Port Security

This chapter contains the procedures for setting port security. The sections in this chapter include:

- ❑ **Port Security Overview** on page 76
- ❑ **Configuring Port Security** on page 78
- ❑ **Configuring the Limited Security Mode** on page 80

Note
Port security does not apply to ports on GBIC modules in an AT-8024GB switch.

Note
Port security can only be set through a local management session, You cannot set port security from a Telnet, Web, or SNMP management session.

Port Security Overview

The port security feature can enhance the security of your network. You can use the feature to control the number of MAC addresses learned on the ports, and so control the number of network devices that can forward frames through the switch.

There are four levels of port security. Only one security level can be active on a switch at a time.

Automatic
This operating mode disables port security. The switch learns and adds addresses to its dynamic MAC address table as it receives frames on the ports. The switch continues to learn MAC addresses so long as there is space in the MAC address table and deletes inactive MAC addresses.

> **Note**
> The Automatic security mode is the default security level for the switch.

Limited
You can use this security level to manually specify a maximum number of dynamic MAC addresses each port on the switch can learn. Once a port has learned its maximum limit, it discards frames that ingress the port with source MAC addresses not already stored in the MAC address table.

Once this mode is activated, the switch deletes all MAC addresses in the dynamic MAC address table and immediately begins learning new addresses, adding them to the dynamic MAC address table for each port until it reaches the port's maximum limit.

The MAC aging time is disabled under this security level. Once a dynamic MAC address has been learned on a port and added to the MAC address table, it remains in the table and is never purged, even when the end node is inactive.

> **Note**
> Static MAC addresses are retained by the switch and are not included in the count of maximum addresses that can be learned by a port. You can continue to add static MAC addresses to a port even if the port has already learned its maximum number of dynamic MAC addresses.

Secure
This security level instructs the switch to forward frames based solely on static MAC addresses. When this security level is activated, the switch deletes all dynamic MAC addresses and disables the MAC address table so that no new addresses can be learned.

The switch also deletes any addresses in the static MAC address table. Once you have activated this security level, you must enter the static MAC addresses of the nodes whose frames the switch should forward. The switch will forward frames only from those nodes whose MAC addresses you enter in the static MAC address table. Any node whose MAC address is not in the static MAC address table will not be able to send frames through the switch.

Lock All Ports
This security level causes the switch to immediately stop learning new dynamic MAC addresses. The switch forwards frames based on the dynamic MAC addresses that it has already learned and any static MAC addresses that the network administrator has entered.

The MAC aging time is disabled in this security level; no dynamic MAC addresses are deleted from the MAC address table, even those belonging to inactive end nodes.

Note
For background information on MAC addresses and aging time, refer to **MAC Address Overview** on page 162.

Configuring Port Security

Note
Port security can only be set through a local management session. You cannot set port security from a Telnet management session or from a web browser management session.

To set a switch's port security level, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **5** to select Port Security.

   The Port Security menu in Figure 17 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                  Port Security


1 - Configure Port Security Mode ....... AUTOMATIC
2 - Configure Limited Mode Parameters

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 17 Port Security Menu

3. Type **1** to select Configure Port Security Mode.

   The following prompt is displayed:

```
Enter new mode (A-Automatic, L-Limited, S-Secured, K-
locKed) :
```

4. Select the desired security level by typing the corresponding letter:

   - To disable port security on the switch, type **A** to select Automatic mode. A switch operating in Automatic mode does not restrict the number of MAC addresses learned by the ports. The switch continues to learn addresses so long as there is available space in the MAC address table. This is the default setting.
   - To specify a maximum number of MAC addresses each port can learn, type **L** to select Limited mode. To specify the limits, perform the procedure in **Configuring the Limited Security Mode** on

page 80.

- To forward frames based solely on static MAC addresses, type **S** to select the Secured mode. After activating this security mode, you must enter the static MAC addresses of the nodes with frames the switch is to forward. For instructions on how to add static MAC addresses, refer to **Adding Static and Multicast MAC Addresses** on page 171.
- To stop the switch from learning new dynamic MAC addresses and have it forward frames based only on static MAC addresses and on those dynamic addresses that it has already learned, type **K** to select Lock all the ports now.

Note
Only one security level can be active on a switch at a time.

A change to the security level is immediately activated on the switch.

Configuring the Limited Security Mode

The Limited security mode lets you set a maximum number of dynamic MAC addresses each port on a switch can learn. When you activate this security level, the switch deletes all MAC addresses in the dynamic MAC address table and immediately begins to learn new addresses as frames are received on the ports. Once the maximum number of MAC addresses have been learned by a port, frames with new source MAC addresses are discarded and are not forwarded.

You can assign the same limit to all ports or different limits to different ports.

Static MAC addresses are not deleted from the static MAC address table. Static MAC addresses are not included in the count of the maximum MAC addresses a port can learn. You can continue to add static MAC addresses even after a port has learned its maximum number of dynamic MAC addresses.

To configure Limited security mode, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **5** to select Port Security.

   The Port Security menu in Figure 17 on page 78 is displayed.
3. From the Port Security menu, type **2** to select Configure Limited Mode Parameters.

   The Limited Security Mode menu in Figure 18 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
         Port Security Limited-Mode Menu


1 - Display MAC Limits
2 - Configure Limited Mode Parameters

R - Return to Previous Menu

Enter your selection?
```

Figure 18 Limited Security Mode Menu

4. Type **2** to select Configure Limited Mode Parameters.

   The following prompt is displayed:

   ```
   Enter ports list:
   ```

5. Enter the port(s) where you want to specify a new MAC address limit. You can specify the ports individually (e.g., 1,4), as a range (e.g., 4-7), or both (e.g., 2-7,11,15).

   The following prompt is displayed:

   ```
   Enter new MAC limit ->  [1 to 150] ->
   ```

6. Enter the maximum number of dynamic MAC addresses you want the port to be able to learn and press Return. The range is 1 to 150 addresses. The default is 100.
7. Repeat this procedure starting with Step 4 to specify MAC address limits on other ports.
8. Type **S** to select Save Configuration Changes.
9. Type **1** to select Display MAC Limits.

   The current MAC address limits for all ports are displayed.

10. Examine the MAC limits. Check to be sure that they are correct. If you assigned different values to different ports, be sure that the different values apply to the correct ports. If necessary, repeat this procedure to change any MAC address limits.

Chapter 7
Port Trunking

This chapter contains the procedures for creating and deleting port trunks. Sections in the chapter include:

- ❑ **Port Trunking Overview** on page 83
- ❑ **Creating a Port Trunk** on page 89
- ❑ **Deleting a Port Trunk** on page 91

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between two Ethernet switches. A port trunk is 2, 3, or 4 ports that have been grouped together to function as one logical path. A port trunk increases the bandwidth between switches and is useful in situations where a single physical data link between switches is insufficient to handle the traffic load.

A port trunk always sends packets from a particular source to a particular destination over the same link within the trunk. A single link is designated for flooding broadcasts and packets of unknown destination.

The example in Figure 19 consists of a port trunk of four data links between two AT-8024 switches.

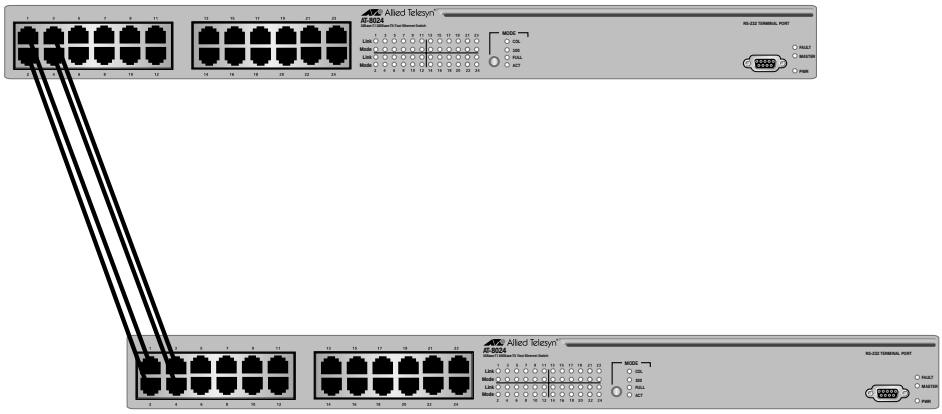

Figure 19 Port Trunk Example

Observe the following guidelines when creating a port trunk:

- An AT-8000 Series switch can support only one port trunk at a time.
- A port trunk can consist of 2, 3, or 4 ports.
- The ports of a port trunk must be of the same medium type. For example, they can be all twisted pair ports or all fiber optic ports.
- The speed, duplex mode, and flow control settings must be the same for all the ports in a trunk.
- The ports of a port trunk must be members of the same VLAN. A port trunk cannot consist of ports from different VLANs.

- When cabling a trunk, the order of the connections should be maintained on both nodes. The lowest numbered port in a trunk on the switch should be connected to the lowest numbered port of the trunk on the other device, the next lowest numbered port on the switch should be connected to the next lowest numbered port on the other device, and so on.

  For example, assume that you are connecting a trunk between two AT-8024 switches. On the first AT-8024 switch you had chosen ports 12, 13, 14, 15 for the trunk. On the second AT-8024 switch you had chosen ports 21, 22, 23, and 24. To maintain the order of the port connections, you would connect port 12 on the first AT-8024 switch to port 21 on the second AT-8024, port 13 to port 22, and so on.

- You can create a port trunk of optional GBIC modules installed in Port 25 and Port 26 of an AT-8024GB switch.

- You can create a port trunk of the fiber optic ports in an AT-8026FC switch.

- You can create a port trunk of the ports in two expansion modules in an AT-8016F switch, providing that the ports are of the same medium type and have the same operating specifications.

Load Distribution Methods

There are two steps to creating a port trunk. The first is to identify the ports on the switch that are to function as the port trunk. The second is to select a load distribution method. This second step is important because unless you select the correct distribution method for your configuration, the switch might not evenly distribute the load across all the links of a trunk. Naturally, this could greatly diminish the value and purpose of the port trunk.

The AT-S39 management software offers two load distribution methods. They are:

- Source Address (SA) Trunking

- Source Address / Destination Address (SA/DA) Trunking

Let's first take a look at the SA method. When a switch receives a packet from a network node, it examines the destination address to determine on which switch port, if any, the packet should be transmitted. If the packet is destined for a port trunk, the switch then examines the source address of the packet. If this is the first packet from the source node to be transmitted over a port trunk, the switch assigns the source address to one of the trunk links. All subsequent packets from the source node are sent out the assigned data link of the trunk.

The switch assigns source addresses so as to evenly distribute the addresses, or at least as much as possible, across all the ports of the trunk. The intent is to try and ensure that all links in the trunk are utilized.

Here is an example. Figure 20 shows two AT-8000 Series Switches, an AT-8024 (Switch #1) and an AT-8024GB (Switch #2) interconnected with a port trunk of three data links. The trunk on Switch #1 consists of Ports 13 to 15 and on Switch #2 of Ports 1 to 3. The 10Base and 100Base workstations are directing traffic to a server connected to Switch #2. The server is connected to Switch #2 with a fiber optic Gigabit Ethernet data link provided by a 1000Base fiber optic GBIC module in the AT-8024GB switch.

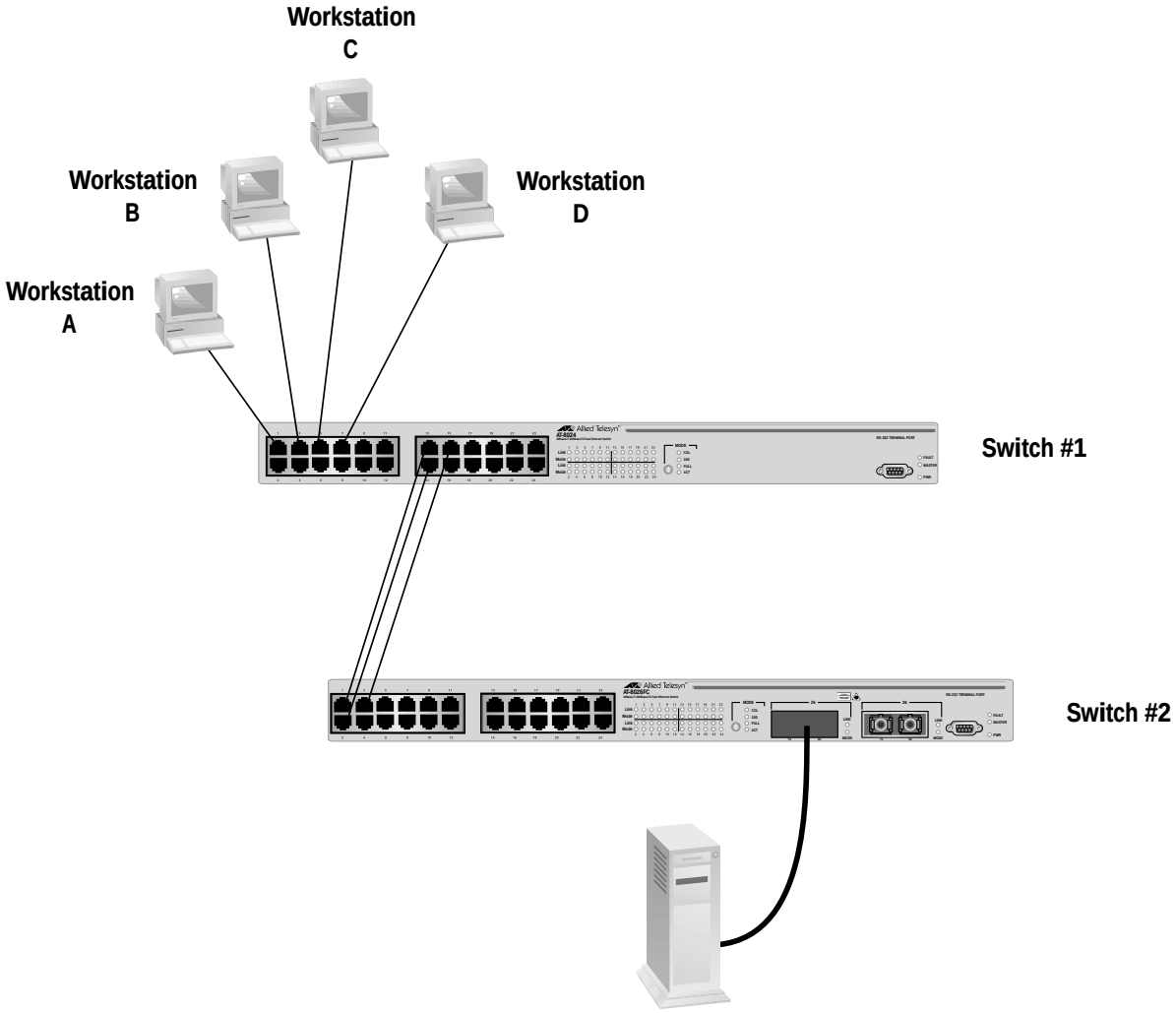

Figure 20 Load Distribution Method

Now assume that you configured the port trunk on Switch #1 for SA load distribution. The switch might distribute the load as follow:

Table 1 Switch #1 Load Distribution

Source Workstation	Source MAC Address	Trunk Port
A	00A0EE 2313A3	13
B	00A134 1A9032	14
C	00A301 9083B2	15
D	001B21 87C6D6	14

For example, when Workstation B sends a packet to the server, Switch #1 will use Port 14 of the trunk to transmit it to Switch #2.

An assignment of a source MAC address to a port trunk remains active as long as the source node remains active. If the MAC address times out, the assignment is dropped. Should the source node become active again and need to transmit a packet over the trunk, a new assignment is made, either to the same port or to a different port in the trunk.

It should be noted that packets sent back from the destination node to the original source node may travel the same or a different data link in the trunk.

As a general rule, the SA load distribution method is useful in situations where the number of source nodes equals or is greater than the number of data links in the trunk.

So when would the SA method be inappropriate? Let's look back again at the example in Figure 20. Let's assume that you configured Switch #2 also for SA load distribution. The result would be that the switch would use only one data link in the trunk to send packets back to Switch #1, because there is only one source, a Gigabit Ethernet server, connected to Switch #2. Since there is only one source, only one data link is used. So obviously the SA method is not appropriate when there are fewer source nodes than data links.

So now let's look at the SA/DA method. A switch using the SA/DA method creates a matrix of the source and destination MAC addresses and then uses the matrix to determine which port in the trunk a frame is to be transmitted. With this method, packets from a particular source node might be sent over different data links in a trunk when sent to different destination addresses.

So let's take a look at how this might look in practice. Assume that you configured Switch #2 in our example for SA/DA. The result might be something similar to that shown in Table 2.

Table 2 Trunk Port Assignments in an SA/DA Matrix

	Destinations MAC Addresses			
Source MAC Address	Workstation A 00A0EE 2313A3	Workstation B 00A134 1A9032	Workstation C 00A301 9083B2	Workstation D 001B21 87C6D6
Server 00B012 DA0231	2	1	3	1

Even though there is only one source, all the data links in the trunk are used. For instance, if the server needed to send a packet to Workstation C, by referring to the matrix Switch #2 would use Port 3 of the trunk to transmit the packet from that particular source MAC address to Switch #1.

As you can see, the SA/DA method is useful when a port trunk needs to send packets from one source node to many destination nodes, something that the SA method is not suited for. Additionally, the SA/DA method is also valid when sending from many source nodes to one destination node, or from many sources to many destinations.

The table below shows a possible matrix for a port trunk of three data links using the SA/DA method, handling traffic from four sources to four destinations.

Table 3 Trunk Port Assignments in an SA/DA Matrix

	Destinations Addresses			
Source Addresses	**00A0EE 2313A3**	**00A134 1A9032**	**00A301 9083B2**	**001B21 87C6D6**
00B012 DA0231	1	2	3	1
001230 DA2943	2	3	1	2
0042AA D45A21	3	1	2	3
00456A C23521	1	2	3	1

The bottom line is that the SA/DA method is more flexible than the SA method. A general rule to follow is if you are not sure which load distribution to choose, you should probably go with SA/DA.

Creating a Port Trunk

This section contains the procedure for creating a port trunk on the switch. Be sure to review the guidelines in **Port Trunking Overview** on page 83 before performing the procedure.

Caution
Do not connect the cables to the trunk ports on the switches until after you have configured the trunk with the management software. Connecting the cables before configuring the software will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

Note
Before creating a port trunk, examine the parameter settings of the ports that will make up the trunk. Check to be sure that the settings, such as speed and duplex mode, are the same for all the ports of the trunk. You should also check to be sure that the ports are members of the same VLAN.

To create a port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **3** to select Port Trunking.

   The Port Trunking menu in Figure 21 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                  Port Trunking


1 - Trunk Ports ..... None

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 21 Port Trunking Menu

3. Type **1** to select Trunk Ports.

   The following prompt is displayed.

   ```
   Enter Trunk Port(s) ->
   ```

4. Enter the ports that will constitute the port trunk and press Return.

   You can specify the ports individually (e.g., 1,2,3,4) or as a range (e.g., 7-10).

   Once you have specified the ports of the trunk, the following menu selection appears:

   ```
   2 - Trunk Method ....... SA/DA trunking
   ```

   You can use this selection to specify the load distribution method. The default is SA/DA.

5. To change the load distribution method, type **2** to toggle the selection through its possible settings of SA/DA and SA only trunking. The change in Port Trunking configuration is immediately activated on the switch.
6. Type **S** to select Save Configuration Changes.
7. Configure the ports on the remote switch for port trunking.
8. Connect the cables to the ports of the trunk on the switch.

   The port trunk is ready for network operation.

Deleting a Port Trunk

Caution
Disconnect the cables from the port trunk on the switch before performing the following procedure. Deleting a port trunk without first disconnecting the cables can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

To delete a port trunk from the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **3** to select Port Trunking.

   The Port Trunking menu in Figure 21 on page 89 is displayed.
3. Type **D** to select Delete trunk.

   A confirmation prompt is displayed.
4. Type **Y** for yes to delete the port trunk or **N** for no to cancel this procedure.

   The deletion of the port trunk is immediately activated on the switch.
5. Type **S** to select Save Configuration Changes.

Chapter 8
Port Mirroring

This chapter contains the procedures for creating and deleting a port mirror. Sections in the chapter include:

- ❑ **Port Mirroring Overview** on page 93
- ❑ **Creating a Port Mirror** on page 94
- ❑ **Deleting a Port Mirror** on page 95

Port Mirroring Overview

The port mirroring feature allows you to unobtrusively monitor the traffic being received and transmitted on one or more ports on a switch by having the traffic copied to another switch port. You can connect a network analyzer to the port where the traffic is being copied and monitor the traffic on the other ports without impacting network performance or speed.

Observe the following guidelines when creating a port mirror:

- ❑ You can mirror from one to 23 ports on a switch at a time. However, the more ports you mirror, the less likely the mirroring port will be able to handle all the traffic. For example, if you mirror the traffic of six heavily active ports, the mirror port is likely to drop packets, meaning that it will not provide an accurate mirror of the traffic of the other six ports.
- ❑ The ports to be mirrored and the mirroring port must be located on the same switch.
- ❑ The ports to be mirrored and the mirroring port must be operating at the same speed. For example, you cannot use a 10/100 Mbps port to mirror traffic on a 1000 Mbps GBIC port.

Creating a Port Mirror

To create a port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **2** to select Port Mirroring.

   The Port Mirroring menu in Figure 22 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                 Port Mirroring


1 - Mirror (Destination) Port ....... None
2 - Mirroring (Source) Port(s) ...... None

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 22 Port Trunking Menu

3. Type **1** to select Mirror (Destination) Port.

   The following prompt is displayed.

   ```
   Enter Mirror port (0=None) [0 to 24] ->
   ```

4. Enter the number of the port to function as the mirror port (that is, the port to where the traffic will be copied). Press Return.

   You can specify only one mirror port.

5. Type **2** to select Mirroring (Source) Port.

   The following prompt is displayed.

   ```
   Enter Mirroring Ports (0=None):
   ```

6. Enter the number of the port whose traffic is to be mirrored. To mirror the traffic of more than one port, enter the ports individually (e.g., 1,4,6) or as a range (e.g., 11-14). Press Return.
7. Type **S** to select Save Configuration Changes.

   The port mirror is now functional.

Deleting a Port Mirror

To delete a port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **2** to select Port Mirroring.

   The Port Mirroring menu in Figure 22 on page 94 is displayed.
3. Type **1** to select Mirror (Destination) Port.

   The following prompt is displayed.

   ```
   Enter mirror port (0=None) [0 to 24] ->
   ```
4. Enter **0** and press Return.
5. Type **S** to select Save Configuration Changes.

   The port mirror on the switch is deleted. The port that was functioning as the port mirror is now available for normal network operations.

Chapter 9
STP and RSTP

This chapter provides background information on the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). The chapter also contains procedures on how to adjust the STP and RSTP bridge and port parameters. The sections in this chapter include:

- **STP and RSTP Overview** on page 97
- **Enabling or Disabling STP or RSTP** on page 105
- **Configuring STP** on page 106
- **Configuring RSTP** on page 110

Note
For detailed information on the Spanning Tree Protocol, refer to IEEE Std 802.1d. For detailed information on the Rapid Spanning Tree Protocol, refer to IEEE Std 802.1w.

STP and RSTP Overview

A significant danger to Ethernet network performance is the existence of a data loop in a network topology. A data loop exists when two or more nodes on a network can transmit data to each other over more than one data link. The problem that data loops pose is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and significantly reduce network performance.

STP and RSTP prevent data loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode, leaving only one main active path.

STP and RSTP can also activate a redundant path if the main path goes down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating a backup redundant path in case a main link fails.

Where the two protocols differ is in the time each takes to complete the process commonly referred to as *convergence*. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain intercommunications between the various network segments. This process is referred to as convergence.

With STP, convergence can take minutes to complete in a large network. This can result in lost data packets and the loss of intercommunication between various parts of the network during the convergence process.

RSTP is much faster. Rather than taking minutes, RSTP can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network.

Note
RSTP is activated by default on the switch.

The STP implementation on the AT-8000 Series Switch complies with the IEEE 802.1d standard. The RSTP implementation complies with the IEEE 802.1w standard. The following subsections provide a basic overview on how STP and RSTP operate and define the different parameters that you can adjust.

Bridge Priority and the Root Bridge

The first task that bridges perform when a spanning tree protocol is activated on a network is the selection of a *root bridge*. A root bridge distributes network topology information to the other network bridges and is used by the other bridges to determine if there are redundant paths in the network.

A root bridge is selected by a combination of a *bridge priority* number, also referred to as the bridge identifier, and sometimes the bridge's MAC address. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

The bridge priority number can be changed on an AT-8000 Series switch. You can designate which switch on your network you want as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge off-line, and assign that bridge the second lowest bridge identifier number.

With STP, the bridge priority has a range of from 0 to 65535. You can select any value within that range.

With RSTP, the range is slightly less, from 0 to 61440. Furthermore, you can only select a value that is a multiple of 4096. To make this easier for you, the management software divides the range into increments. You specify the increment that represents the desired bridge priority value. The range is divided into sixteen increments, as shown in the following table.

Table 4 RSTP Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Path Costs and Port Costs

Once the Root Bridge has been selected, the bridges must determine if the network contains redundant paths and, if one is found, they must select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and the root bridge, the bridge is referred to as the *designated bridge* and the port through which the bridge is communicating with the root bridge is referred to as the *root port*.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by an determination of *path costs*. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed into blocking state.

Path cost is determined through an evaluation of *port costs*. Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is simply the cumulation of the port costs between a bridge and the root bridge.

The port costs of the ports on an AT-8000 Series switch are adjustable through the management software, but the range is different depending on whether you are using STP or RSTP.

For STP, the range is 1 to 65535. You can assign a port a port cost of any value within the range. Below are the default values.

Table 5 STP Default Port Costs

Port Speed	Port Cost
10 Mbps	10
100 Mbps	10
1000 Mbps	4

In RSTP, the range is much greater: 0 to 20 000 000. This greater range allows you to have more control over path costs.

RSTP port cost also features an Auto-Detect feature. This features allows RSTP to automatically set the port cost according to the speed of the port, assigning a lower value for higher speeds. Auto-Detect is the default setting on the ports when the switch is operating in RSTP. Table 6 lists the ports cost with Auto-Detect.

Table 6 RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2 000 000
100 Mbps	200 000
1000 Mbps	20 000

You can override Auto-Detect and set the port cost manually.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the *port priority* parameter. This parameter can be used as a tie-breaker when two paths have the same cost.

In STP, the range for port priority is 0 to 255.

In RSTP, the range is 0 to 240. As with RSTP Bridge Priority, this range is broken into increments, in this case multiples of 16. When you specify a port priority for a port, you enter the increment of the desired value.

Table 7 RSTP Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Forwarding Delay and Topology Changes

If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It might take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. If a topology change is made before all bridges have been notified, a temporary data loop could occur, and that could adversely impact network performance.

To forestall the formation of temporarily data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states, listening and learning, before it begins to forward frames. The amount of time a port spends in these states is set by the *forwarding delay* value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The forwarding delay value is adjustable on the AT-8000 Series switch through the management software. The appropriate value for this parameter will depend on a number of variables, with the size of your network being a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should not specify a value so large that a topology change is unnecessarily delayed, which could result in the delay or loss of some data packets.

Note
The forwarding delay parameter applies only to STP.

Hello Time and Bridge Packet Data Units (BPDU)

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the Bridge Packet Data Unit (BPDU). When a bridge is brought on-line, it will issue a BPDU in order to determine whether a root bridge has already been selected on the network. and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge will periodically transmit a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the *Hello Time*. This is a value that you can set on the AT-8000 Series switch. The interval is measured in seconds and the default is 2 seconds. Consequently, if an AT-8000 Series switch is selected as the Root Bridge of a spanning tree domain, it will transmit a BPDU every two seconds.

Point-to-Point Ports and Edge Ports

> **Note**
> This section applies only to RSTP.

Part of the task of configuring RSTP is defining the port types on the bridge. This relates to the device(s) connected to the port. With port type defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

There are two possible selections:

- Point-to-point
- Edge port

If a bridge port is operating in full-duplex mode, than the port is functioning as point-to-point. Figure 23 illustrates two AT-8024 switches that have been interconnected with one data link. With the link operating in full-duplex, the ports are said to be point-to-point ports.

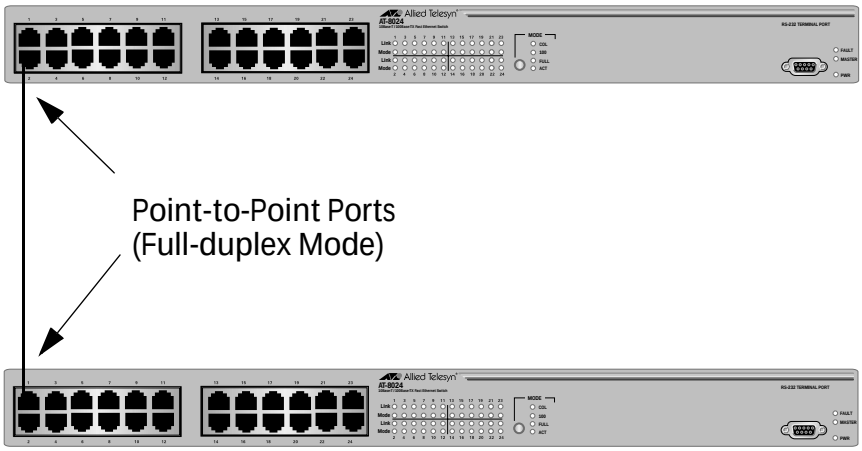

Figure 23 Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any further bridges participating in STP or RSTP, then the port is an edge port. Figure 24 illustrates an edge port on an AT-8024 switch. The port is connected to an Ethernet hub, which in turn is connected to a series of Ethernet workstations. This is an edge port because it is connected to a device operating at half-duplex mode and there are no participating STP or RSTP devices connected to it.

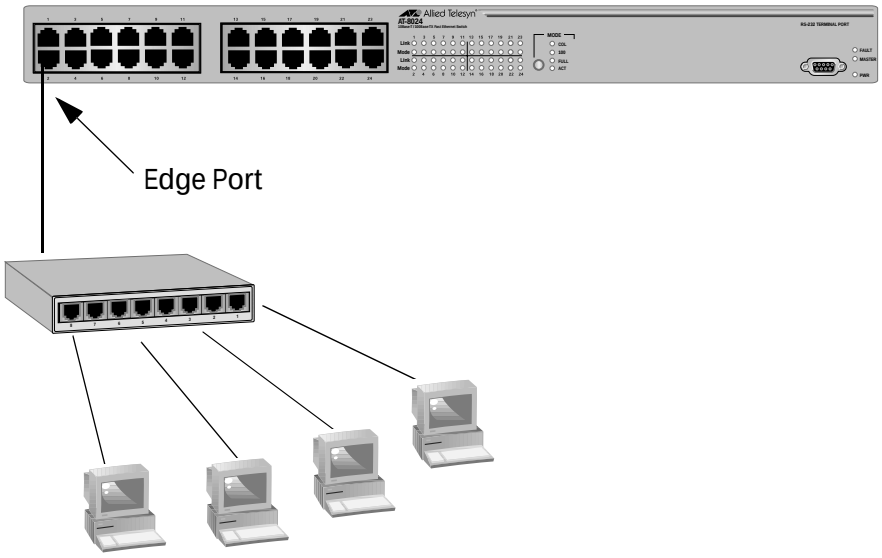

Figure 24 Edge Port

A port can be both point-to-point and edge at the same time. It would operate in full-duplex and have no STP or RSTP devices connected to it. Figure 25 illustrates a port functioning both as point-to-point and edge.

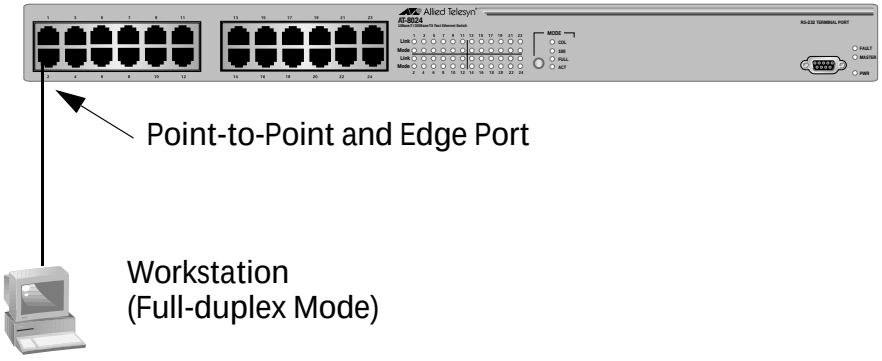

Figure 25 Point-to-Point and Edge Point

Determining whether a bridge port is point-to-point, edge, or both, can be a bit confusing. For that reason it might be best not to change the default values for this RSTP feature unless in have a good grasp of the concept. In most cases, the default values will work fine.

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. Your network can consist of bridges running both protocols. STP and RSTP in the same network should be able to operate together to create a single spanning tree domain.

There is no reason not to activate RSTP on an AT-8000 Series switch even when all other switches are running STP. The AT-8000 Series switch can combine its RSTP with the STP of the other switches. An AT-8000 Series switch will monitor the traffic on each port for BPDU packets. Ports that receive RSTP BPDU packets will operate in RSTP while ports receiving STP BPDU packets will operate in STP.

Spanning Tree and VLANs

The spanning tree implementation on an AT-8000 Series switch is a single-instance spanning tree. The switch supports just one spanning tree. You cannot define multiple spanning trees.

The single spanning tree encompasses all ports on the switch. If the ports are divided into different VLANs, the spanning tree crosses the VLAN boundaries. This point can pose a problem in networks containing multiple VLANs that span different switches and are connected with untagged ports. What can happen is that STP will block a data link because it detects a data loop. This can cause fragmentation of your VLANs.

This issue is illustrated in Figure 26. Two VLANs, Sales and Production, span two AT-8024GB switches. Two links consisting of untagged ports interconnect the separate parts of each VLAN. If STP is activated on the switches, one of the links would be disabled. This problem can be avoided by not activating spanning tree or by connecting VLANs using tagged instead of untagged ports. (For information on tagged and untagged ports, refer to **Chapter 10, Virtual LANs Overview** on page 115.

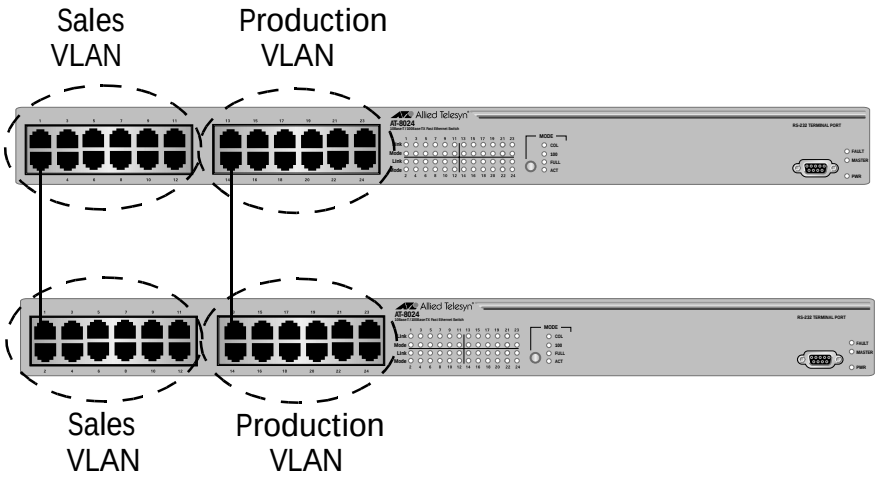

Figure 26 VLAN Fragmentation

Enabling or Disabling STP or RSTP

To select and activate a spanning tree protocol, or to disable spanning tree, perform the following procedure:

1. From the Main Menu, type **3** to select Spanning Tree Menu.

   The Spanning Tree Menu in Figure 27 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
               Spanning Tree Menu
1 - Spanning Tree Status ..... Disabled
2 - Active Protocol Version ... RSTP
3 - STP Configuration
4 - RSTP Configuration

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 27 Spanning Tree Menu

2. To enable or disable spanning tree, type **1** to select Spanning Tree Status.
3. Type **E** to enable spanning tree or **D** to disable it. The default is enabled.
4. To change the version of spanning tree protocol running on the switch, type **2** to select Active Protocol Version.

   Note
   Changing the spanning tree version will reboot the switch.

   The following prompt is displayed:

```
The switch will be rebooted for changing the
protocol version.
Do you want to continue? [Yes/No]
```

5. Type **Y** for yes to change the current version of spanning tree and reboot the switch, or **N** to cancel this procedure.
6. If you activated spanning tree and you selected STP, go to **Configuring STP** on page 106 for further instructions. If you selected RSTP, go to **Configuring RSTP** on page 110

Configuring STP

This section contains the following procedures:

- ❑ **Configuring a Bridge's STP Settings** on page 106
- ❑ **Configuring a Port's STP Settings** on page 108

Configuring a Bridge's STP Settings

This section contains the procedure for configuring a bridge's STP settings.

Caution
The default STP parameters are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

1. From the Spanning Tree Menu, type **3** to select STP Configuration.

   The STP Menu in Figure 28 is displayed.

```
     Allied Telesyn AT-8024 Ethernet Switch
Login Privilege: Manager
                    STP Menu
The current protocol version is STP.
1 - Bridge Priority ..... 65535
2 - Bridge Hello Time ... 2
3 - Bridge Forwarding ... 15
4 - Bridge Max Age ...... 20

6 - Config STP Port Settings
7 - Display STP Port Settings
8 - Reset STP to Defaults

R - Return to Previous Menu


Enter your selection?
```

Figure 28 STP Menu

2. Adjust the bridge STP settings as needed. The parameters are described below.

   1 - Bridge Priority
   The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 65,535, with 0 being the highest priority.

   2 - Bridge Hello Time
   The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

   3 - Bridge Forwarding
   The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The default is 15 seconds.

   4 - Bridge Max Age
   The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

   In selecting a value for maximum age, the following must be observed:

   MaxAge must be less then (2 x (HelloTime + 1)).

   MaxAge must be less then (2 x (ForwardingDelay - 1)).

   Note
   The aging time for BPDUs is different from the aging time used by the MAC address table.

3. After you have made the desired changes, type **S** to select Save Configuration Changes.
4. To change STP port settings, go to the next procedure.

Configuring a Port's STP Settings

To adjust a port's STP parameters, perform the following procedure:

1. From the Spanning Tree Menu, type **3** to select STP Configuration.
2. From the STP Configuration menu, type **6** to select Config STP port settings.

   The following prompt is displayed:

   ```
   Starting Port to Configure [1 to 24] ->
   ```
3. Enter the number of the port you want to configure. To configure a range of ports, enter the first port of the range.

   The following prompt is displayed:

   ```
   Ending Port to Configure [1 to 24] ->
   ```
4. To configure just one port, enter the same port number here as you entered in the previous step. To configure a range of ports, enter the last port of the range.

   The STP Port Configuration menu in Figure 29 is displayed.

```
Allied Telesyn AT-8024 Ethernet Switch
Login Privilege: Manager
              Config STP Port Settings

Configuring Ports 4 to 4
1 - Participate ....... Yes
2 - Fast Mode ......... No
3 - Port Cost ......... Automatic Update
4 - Port Priority ..... 128
5 - Port State ........ Disabled
6 - Root Bridge .......

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 29 Config STP Port Settings Menu

5. Adjust the settings as desired. The parameters are described below.
6. After adjusting the parameters, type ***S*** to select *Save Configuration Changes.*

Note
A change to the port priority parameter takes effect immediately. A change to the port cost value requires youto reset the switch. A new port cost value is not implemented until the unit is reset.

1 - Participating
This selection activates and deactivates STP on the port. If set to Yes, which is the default, the port will participate in the spanning tree. If you select No, the port will continue to receive and transmit Ethernet frames, but it will not participate in spanning tree.

Note
A port on which STP is disabled is immediately placed in the forwarding state. It should be noted that a port where STP has been disabled cannot be placed in the blocking state by STP should there be a loop in the network topology. Consequently, it is incumbent on the network administrator to insure that no loop will develop should STP be disabled on a port.

2 - Fast Mode
The port will skip the Listening and Learning stages of STP. This setting is appropriate for ports connected to edge nodes that are not running STP.

3 - Port Cost
The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The default value for this parameter for all ports and speeds is 100. The range is 1 to 65535. To automatically set a port's STP port cost based on port speed, set the value to a "0".

4 - Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The default value for priority is 128. The range is 0-255.

5 - Port State
The current STP status of the port. The status can be Forwarding, Listening, Learning, or Blocking. This value cannot be changed.

6 - Root Bridge
The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for display purposes only and cannot be changed.

Configuring RSTP

This section contains the following procedures:

- ❑ **Configuring a Bridge's RSTP Settings** on page 110
- ❑ **Configuring a Port's RSTP Settings** on page 112

Configuring a Bridge's RSTP Settings

This section contains the procedure for configuring a bridge's RSTP settings.

> ⚠ **Caution**
> The default RSTP parameters are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

1. From the Spanning Tree Menu, type **4** to select RSTP Configuration.

   The RSTP Menu in Figure 30 is displayed.

```
Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                     RSTP Menu
The current protocol version is RSTP

1 - Force Version .......... RSTP
2 - Bridge Priority ........ 32768
3 - Bridge Hello Time ...... 2
4 - Bridge Forwarding ...... 15
5 - Bridge Max Age ......... 20
6 - Bridge Identifier ...... 00:30:84:52:03:80

P - RSTP Port Parameters
D - Reset RSTP to Defaults

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 30 RSTP Menu

2. Adjust the parameters as needed. The parameters are defined below.

   1 - Force Version
   This selection determines whether the bridge will operate with RSTP or in an STP-compatible mode. If you select RSPT, the bridge will operate all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge will operate in RSTP, using the RSTP parameter settings, but it will send only STP BPDU packets out the ports.

   2 - Bridge Priority
   The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to **Table 4**, **RSTP Bridge Priority Value Increments** on page 98

   3 - Bridge Hello Time
   The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

   4 - Bridge Forwarding
   The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

   5 - Bridge Max Age
   The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

   In selecting a value for maximum age, the following must be observed:

   MaxAge must be less then (2 x (HelloTime + 1)).

   MaxAge must be less then (2 x (ForwardingDelay - 1))

6 - Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

3. After adjusting the parameters, type **S** to select Save Configuration Changes.

Configuring a Port's RSTP Settings

To adjust a port's RSTP parameters, perform the following procedure:

1. From the Spanning Tree Menu, type **4** to select RSTP Configuration.
2. From the RSTP Configuration menu, type **P** to select RSTP Port Parameters.

   The following menu is displayed:

```
Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                RSTP Port Parameters

The current protocol version is RSTP.
1 - Configure RSTP Port Settings
2 - Display RSTP Port Configuration
3 - Display RSTP Port State

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 31 RSTP Port Parameters

3. Type **1** to select Configure RSTP Port Settings.

   The following prompt is displayed:

```
Starting Port to Configure [1 to 24] ->
```

4. Enter the number of the port you want to configure. To configure a range of ports, enter the first port of the range.

   The following prompt is displayed:

```
Ending Port to Configure [1 to 24] ->
```

5. To configure just one port, enter the same port number here as you entered in the previous step. To configure a range of ports, enter the last port of the range.

The RSTP Port Configuration menu in Figure 32 is displayed.

```
       Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
            Configure RSTP Port Settings

Configuring Ports 4 to 4
1 - Port Priority ...... 128
2 - Port Cost .......... Auto Update
3 - Point-to-Point ..... Auto Detect
4 - Edge Port .......... Yes

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 32 Configure RSTP Port Settings Menu

6. Adjust the settings as needed. The parameters are explained below.
7. After making your changes, type ***S*** to select *Save Configuration Changes*.

Note
All changes to a port's RSTP settings, with the exception of port cost, are activated immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

1 - Port Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to **Table 7**, **RSTP Port Priority Value Increments** on page 100.

2 - Port Cost
The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20 000 000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 2 000 000 for 10 Mbps ports, 200 000 for a 100 Mbps ports, and 20 000 for one gigabit ports.

3 - Point-to-Point
This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 102.

4 - Edge Port
This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 102.

After making your changes, type **S** to select Save Configuration Changes.

Chapter 10
Virtual LANs Overview

This chapter contains overviews of AT-S39 management software switch modes and virtual LANs (VLANs).

- **AT-S39 Management Software Switch Modes** on page 116
- **Setting the Switch Mode** on page 117
- **Setting VLAN Status** on page 118
- **VLAN Overview** on page 119
- **User-Configured VLANs** on page 121
- **Tagged VLAN Overview** on page 127
- **Multiple VLAN Mode Overview** on page 132

AT-S39 Management Software Switch Modes

Understanding AT-S39 management software switch modes is essential in understanding VLANs. The AT-S39 software for Fast Ethernet Switches support two switch modes:

- Tagged - the Fast Ethernet Switch supports port-based and tagged VLANs(see ***User-Configured VLANs*** on page 121) or multiple VLAN configuration (see ***Multiple VLAN Mode Overview*** on page 132).

  To skip the VLAN overviews and proceed to VLAN procedures, go to **Configuring User-Created VLANs** on page 137 or **Multiple VLAN Configuration** on page 156.

- Basic - the Fast Ethernet Switch operates in VLAN pass-through mode and frames are forwarded based solely on MAC addresses.

The following two sections describe these switch modes and their relation to VLAN configuration.

Note
For instructions on setting the switch mode, refer to **Setting the Switch Mode** on page 117.

Setting the Switch Mode

To configure the switch mode, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. Type **2** to select Switch Mode.

   The following prompt is displayed:

   ```
   Enter Switch Mode (T-Tagged, B-Basic):
   ```

3. Type **T** to create your own port-based and tagged VLANs, or **B** to configure the switch for the Basic Mode. The default is Tagged mode. Press Return.
4. Type **S** to select Save Configuration Changes.

Setting VLAN Status

In addition to the Switch Mode parameter discussed in the previous section, switch mode status can also be configured in the VLANs menu by enabling or disabling the VLANs Status parameter. When VLANs are enabled, the switch supports Tagged mode. When VLANs are disabled, the switch supports the Basic mode.

The difference between the two procedures has to do with ingress filtering. If you activate the Basic Mode using the Switch Mode parameter in the System Config Menu, ingress filtering is disabled. Changing the VLAN mode using the VLAN Status parameter in the VLANs menu does not change the current setting of ingress filtering.

To configure a switch's VLAN mode using the VLAN Status parameter in the VLANs menu, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **1** to select VLANs Status (the current VLAN status is shown in this menu). The following prompt is displayed:

   ```
   Enter VLAN Status (E-Enable, D-Disable) ->
   ```

3. Type **E** to enable VLAN status, or **D** to disable VLAN status. Press Return.
4. Type **S** to select Save Configuration Changes.

   A change to the VLAN status is immediately activated on the switch.

VLAN Overview

A virtual LAN (VLAN) is a logical grouping of devices on different physical LAN segments that allows users to communicate as if they were physically connected to a single LAN, independent of the physical configuration of the network.

With VLAN switch management software, you can segment your network and group nodes with related functions into their own separate, logical LAN segments. For example, the marketing personnel in your company may be spread throughout a building. Assigning marketing to a single VLAN allows marketing personnel to share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible, or accessible only to specified individuals.

VLAN architecture benefits include:

- ❑ Increased performance
- ❑ Improved manageability
- ❑ Increased security

Increased Performance

In traditional Layer-2 switched environments, broadcast packets are sent to each and every individual port. VLANs address the limitations of standard switch segmentation by containing broadcast as well as node-to-node traffic.

Grouping users into logical networks limits broadcast traffic to users performing similar functions or users within individual workgroups. Extraneous traffic, the danger of broadcast storms, router latency, and data collisions are significantly reduced, and the efficiency of the entire network is improved.

Improved Manageability

VLANs provide a fundamental improvement in the design, administration, and management of LANs. Before the advent of VLANs, physical changes to a network were made at the switch in the wiring closet.

For example, if an employee transferred to a new department, changing that employee's LAN segment assignment often required a physical wiring change at the switch.

As a software-based solution, VLANs eliminate the restrictions of existing network design and cabling infrastructure and allow the centralized configuration of switches located in physically diverse locations. VLAN memberships are changed quickly and efficiently from the management console rather than the wiring closet.

Increased Security

VLANs provide additional security not available in a shared media network environment. Because a switched network only delivers frames to intended recipients, and only broadcasts frames to other members of the VLAN, a network administrator can segment users requiring access to sensitive information into separate VLANs from the rest of the general user community.

Since data traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, VLANs can be used to control the flow of data in your network and prevent data from flowing to unauthorized end nodes.

VLAN Modes

The AT-8000 Series switch supports the following VLAN modes:

- ❑ User-configured VLANs
  - — Port-based
  - — Tagged
- ❑ Multiple VLANs
  - — 802.1Q compliant
  - — non-802.1Q compliant

These VLANs are described in the following sections.

Note
User-configured VLANs are 802.1Q compliant. The only non-802.1Q compliant VLAN mode is non-802.1Q compliant multiple VLAN mode. This mode would generally be used in a network supporting non-802.1Q compliant devices.

User-Configured VLANs

User-configured VLANs are, as the name suggests, VLANs that are manually configured by the user. As mentioned in the previous chapter, there are two types of user-configure VLANs:

- Port-based (discussed in the following section)
- Tagged (see ***Tagged VLAN Overview*** on page 127)

Port-based VLAN Overview

Port-based VLANs are the simplest and most common form of a VLAN. In a port-based VLAN configuration, each port of the switch is assigned to a particular VLAN. Each port can belong to only one port-based VLAN at a time.

For example, you can designate ports 1, 2, and 3 as part of the engineering VLAN and ports 5, 6, and 7 as part of the marketing VLAN.

A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. Additionally, a port-based VLAN can span switches and consist of ports from multiple Ethernet switches.

Note
The AT-8000 Series switch is pre-configured with one port-based VLAN. All ports on the switch are members of this VLAN, called the Default_VLAN.

A port-based VLAN contains the following elements:

- VLAN name
- VLAN Identifier
- Untagged ports
- Port VLAN Identifier

VLAN Name

To create a port-based VLAN, you must give it a name. The name typically reflects the function of the network devices that are members of the VLAN.

VLAN Identifier

Each VLAN in a network requires a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network.

If a VLAN consists only of ports located on one physical switch in your network, you would assign it a VID unique from all other VLANs in your network.

If a VLAN spans multiple switches, the VID for the VLAN on the different switches must be identical. In this manner, the switches are able to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches.

For example, if you had a port-based VLAN titled Marketing that spanned three AT-8024 switches, you would assign the Marketing VLAN on each switch the same VID.

You can assign this number manually or allow the management software to automatically perform this function. If you allow the management software to automatically assign the VID, the next available VID will be selected. If you are creating a VLAN on a switch that is part of a larger VLAN that spans several switches, you must manually assign the number so that the VLAN has the same VID across all switches linked in that VLAN.

Untagged Ports

You must always specify which ports on the switch are members of a port-based VLAN. Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The term *untagged* derives from the fact that the frames received on a port will not contain any information that indicates VLAN membership, and that VLAN membership will be determined solely by the port's PVID.

A port on a switch can be an untagged member of only one port-based VLAN at a time. An untagged port cannot be assigned to two port-based VLANs simultaneously.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to the port on which the frame is received, and forwards the frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. Additionally, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, assume that you were creating a port-based VLAN on a switch and you had assigned the VLAN the VID 5. Consequently, the PVID for each port in the VLAN would need to be assigned the value 5.

Some switches and switch management programs require that you assign the PVID value for each port manually. However, the AT-S39 management software performs this task automatically. The software automatically assigns a PVID to a port, making it identical to the VID of the VLAN to which the port is a member.

General Rules for Creating Port-Based VLANs

Below is a summary of the general rules to observe when creating port-based VLANs.

- Each port-based VLAN must be assigned a unique VID. If a particular VLAN spans multiples switches, each part of the VLAN on the different switches must be assigned the same VID.
- A port can be an untagged member of only one port-based VLAN at a time.
- Each port must be assigned a PVID. This value is assigned automatically by the AT-S39 management software. The value is the same for all ports in a port-based VLAN and is identical to the VLAN's VID.
- A port-based VLAN that spans multiple switches requires a port on each switch where the VLAN is located to function as an interconnection between the switches where the various parts of the VLAN reside.
- If there are end nodes in different VLANs that need to communicate with each other, a router or Layer 3 switch is required to interconnect the VLANs.

Drawbacks to Port-based VLANs

Drawbacks to port-based VLANs:

- Sharing network resources, such as servers and printers, across multiple VLANs can be difficult. A router or Layer 3 switch must be added to the network to provide a means for interconnecting the port-based VLANs. The introduction of a router into the network can create security issues, including unauthorized access to your network.
- A VLAN that spans several switches requires a port on each switch for the interconnection of the various parts of the VLAN. For

example, a VLAN that spans three switches requires one port on each switch to interconnect the various sections of that VLAN.

In network configurations with many individual VLANs that span switches, ports are often ineffectively used to interconnect the various VLANs.

Port-based Example 1

Figure 33 illustrates an example of one AT-8024 Fast Ethernet Switch with three port-based VLANs. (For purposes of the following examples, the Default_VLAN is not shown.)

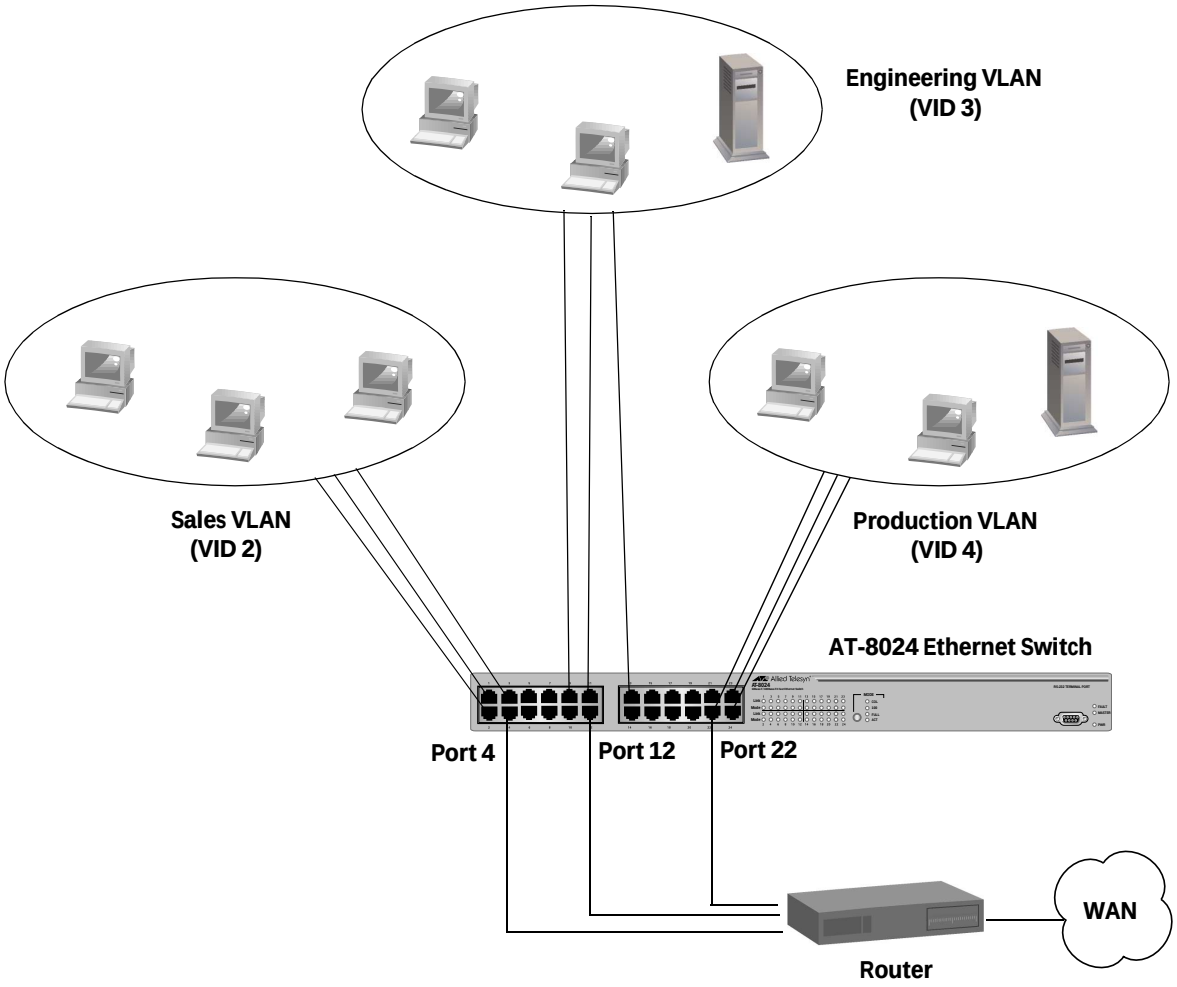

Figure 33 Port-based VLAN - Example 1

The table below lists the port assignments for the Sales, Engineering, and Production VLANs on the switch.

Switch	Sales VLAN (VID 2)	Engineering VLAN (VID 3)	Production VLAN (VID 4)
AT-8024 (top)	Ports 1 - 4 (PVID 2)	Ports 9, 11 - 13 (PVID 3)	Ports 21 - 24 (PVID 4)

Each VLAN has been assigned a unique VID. You assign this number when you create a VLAN.

The ports have been assigned PVID values. A port's PVID is assigned automatically by the management software when you create the VLAN. A PVID is the same as the VID to which the port is an untagged member.

In the example, each VLAN has one port connected to the router. The router interconnects the various VLANs and functions as a gateway to the WAN.

Port-based Example 2

Figure 34 illustrates more port-based VLANs. In this example, two VLANs span more than one Ethernet switch.

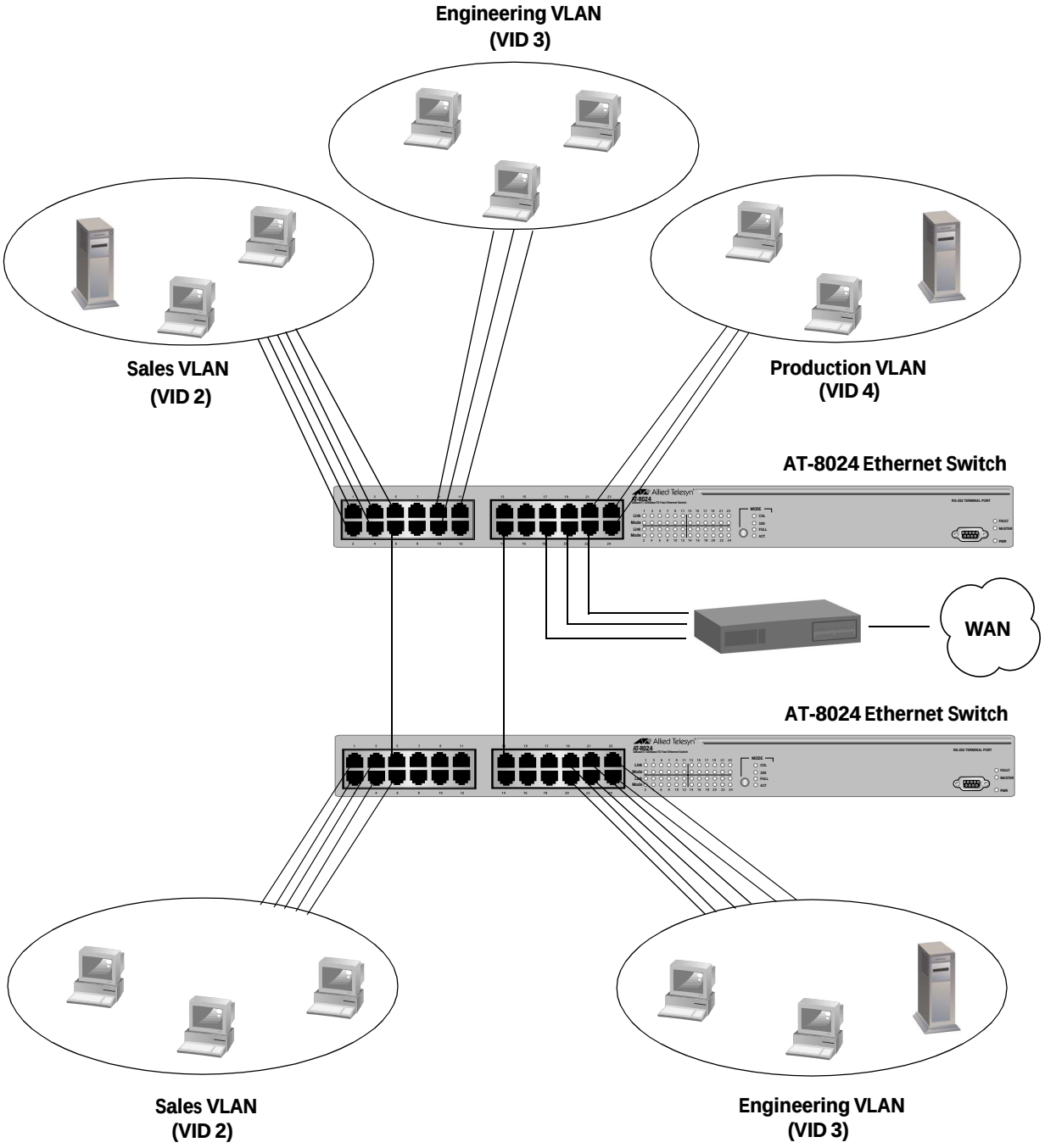

Figure 34 Port-based VLAN - Example 2

The table below lists the port assignments for the Sales, Engineering, and Production VLANs on the switches:

Switch	Sales VLAN (VID 2)	Engineering VLAN (VID 3)	Production VLAN (VID 4)
AT-8024 (top)	Ports 1 - 6, 18 (PVID 2)	Ports 9 - 11, 14, 20 (PVID 3)	Ports 21 - 24 (PVID 4)
AT-8024 (bottom)	Ports 1 - 6 (PVID 2)	Ports 13, 19-24 (PVID 3)	none

- Sales VLAN - This VLAN spans both switches. It has a VID value of 2 and consists of seven untagged ports on the top switch and six untagged ports on the bottom switch.

  The two parts of the VLAN are interconnected by a direct link from Port 6 on the top switch to Port 5 on the bottom switch. This direct link allows the two parts of the Sales VLAN to function as one logical LAN segment.

  Port 18 on the top switch connects to the router. This port allows the Sales VLAN to exchange Ethernet frames with the other VLANs and to access the WAN.

- Engineering VLAN - This port-based VLAN uses Ports 9 to 11 on the top switch and Ports 19 to 24 on the bottom switch as connections to the workstations of the VLAN.

  Since this VLAN spans multiple switches, it needs a direct connection between its various parts to provide a communications path. This is provided in the example with a direct connection from Port 14 on the top switch and Port 13 on the bottom switch.

  This VLAN uses Port 20 on the top switch as a connection to the router and the WAN.

- Production VLAN - This is the final VLAN in the example. It has the VLAN of 4 and its ports have been assigned the PVID also of 4.

  The nodes of this VLAN are connected to only the top switch. So this VLAN does not require a direct connection to the bottom VLAN. However, it uses Port 22 as a connection to the router.

Tagged VLAN Overview

The second type of user-configured VLAN mode supported by the AT-8000 Series switch is the *tagged VLAN*. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This contrasts to a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). As explained earlier in this chapter in **VLAN Identifier** on page 122, this number uniquely identifies each VLAN in a network.

When a tagged port receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID. This is true only when a tagged port is tagged to the destination VLAN.

A port to receive or transmit tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of a tagged VLAN is that the tagged ports within the VLAN can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, a server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch for connecting all VLANs on the switch to another switch.

The IEEE 802.1Q standard deals with how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN that the port is a tagged member of, the frame will be accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs that the port is a member of, the frame will be discarded.

The parts of a tagged VLAN are much the same as those for a port-based VLAN. They are:

- ❑ VLAN Name
- ❑ VLAN Identifier
- ❑ Tagged and Untagged Ports
- ❑ Port VLAN Identifier

Note
For explanations of VLAN name and VLAN identifier, refer back to **VLAN Name** and **VLAN Identifier** on page 122.

Tagged and Untagged Ports

You must specify which ports are members of the VLAN. In the case of a tagged VLAN, VLAN members are usually a combination of both tagged and untagged ports. When you create the VLAN, you specify which ports are tagged and which ports are untagged.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs, simultaneously.

Port VLAN Identifier

As explained earlier in the discussion on port-based VLANs, the management software automatically assigns a PVID to each port when a port is made a member of a VLAN. The PVID is always identical to the VLAN's VID.

Because a tagged port determines VLAN membership by examining the tagged header within the frames that it receives and not by the PVID, it may seem that PVIDs are unnecessary on a tagged port.

While a tagged port's PVID is usually ignored, a tagged port can receive an untagged frame (that is, a frame without any tagged information). In this scenario, the port forwards the untagged frame by using the port's PVID.

General Rules to Creating a Tagged VLAN

Below is a summary of the rules to observe when creating a tagged VLAN.

- ❑ Assign each tagged VLAN a unique VID. If a particular VLAN spans multiple switches or stacks, each part of that VLAN on the different switches or stacks must be assigned the same VID.
- ❑ A tagged port can be a member of multiple VLANs.
- ❑ An untagged port can be an untagged member of only one VLAN at a time.
- ❑ The AT-8000 Series switch can support up to 32 tagged and port-based VLANS.

Tagged VLAN Example

Figure 35 illustrates how tagged ports can be used to interconnect IEEE 802.1Q-based products.

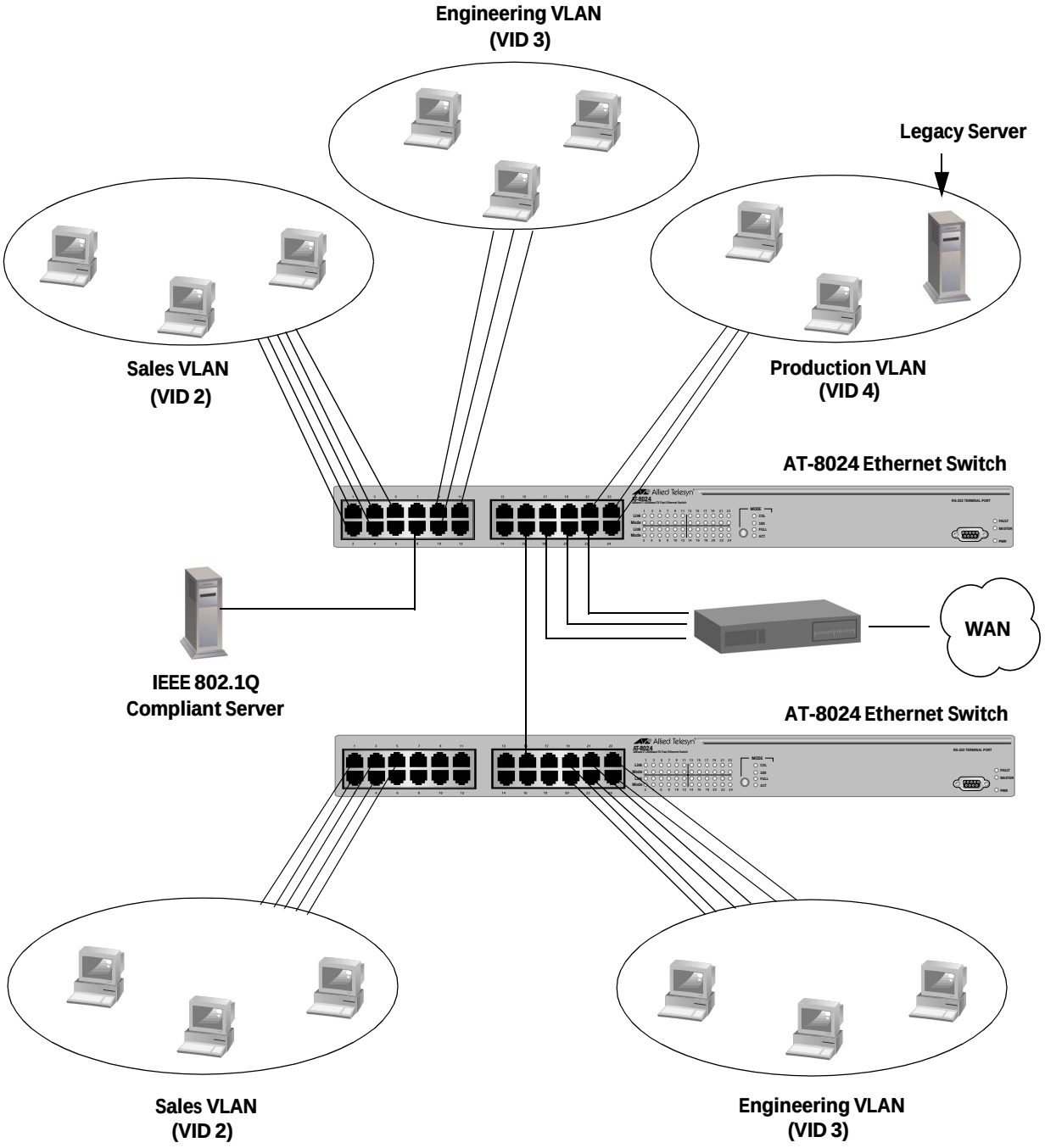

Figure 35 Example of a Tagged VLAN

The port assignments for the VLANs are as follows:

Switch	Sales VLAN (VID 2)		Engineering VLAN (VID 3)		Production VLAN (VID 4)	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
AT-8024 (top)	1 to 5, 18 (PVID 2)	8, 16	9 to 11, 20 (PVID 3)	8, 16	21 to 24 (PVID 4)	8
AT-8024 (bottom)	1 to 5 (PVID 2)	15	19 to 24 (PVID 3)	15	none	none

This example is nearly identical to the **Port-based Example 2** on page 126. Tagged ports have been added to simplify network implementation and management.

Port 8 is a tagged port on the top switch. This port has been made a tagged member of the three VLANs. It is connected to an IEEE 802.1Q-compliant server, meaning the server can handle frames from multiple VLANs. Now all three VLANs can access the server without having to access a router or other interconnection device.

It is important to note that even though the server is receiving and transmitting frames between more than one VLAN, data remains separated and secure.

In the example, Port 16 on the top switch and Port 15 on the bottom switch are tagged ports used to simplify network design. These ports are tagged members of the Sales and Engineering VLANs. These ports provide a connection between the different parts of these two VLANs.

In the **Port-based Example 2** on page 126, each VLAN required its own data link between the switches to connect the different parts of the VLANs. With tagged ports, you can use one data link to carry data traffic from several VLANs, while still maintaining data separation and security. The tagged frames, when received by the switch, are delivered only to those ports that belong to the VLAN from which the tagged frame originated.

Procedures for user-configured VLANs can be found in **Configuring User-Created VLANs** on page 137.

Multiple VLAN Mode Overview

The Multiple VLAN mode simplifies the task of configuring the switch in network environments that require a high degree of network segmentation.

When Multiple VLAN mode is activated, the switch automatically assigns each port as an untagged port to a separate VLAN. Each VLAN is given a unique name and VID number based on the port number. For example, the VLAN for Port 4 is named Client_VLAN_4 and is given the VID of 4, the VLAN for Port 5 is named Client_VLAN_5 and has a VID of 5, and so on.

PVIDs are assigned automatically. For example, the PVID for Port 4 is assigned as 4, to match the VID of 4.

A user-specified port on the switch is designated as an uplink port that can be connected to a shared device, such as a router for access toa WAN. Thus, while the switch ports are separated from each other in their individual VLANs, they all have access to the uplink port.

This highly segmented configuration is useful in situations where traffic generated by each end node or network segment connected to a port on the switch needs to be kept separate from all other network traffic, while allowing access to an uplink to a WAN. Unicast traffic received by the uplink port is effectively directed to the appropriate port and end node, and is not directed to any other port on the switch.

There are two types of Multiple VLAN modes that can be configured using the AT-S39 software:

- ❑ 802.1Q-compliant multiple VLANs (discusssed on page 133)
- ❑ non-802.1Q compliant multiple VLANs (discussed on page 135)

These types of VLANs are discussed in the following sections. Procedures for selecting a multiple VLAN is in **Multiple VLAN Configuration** on page 156.

Note

Multiple VLANs feature is supported only in single switch (i.e. edge switch) environments. This means that cascading of switches while in Multiple VLANs mode is not allowed.

Configuring Multiple VLANs on a cascaded switch can possibly result in disconnection of network paths between switches unless the port used to link the switch (being configured for Multiple VLANs mode) is configured as Uplink VLAN port.

Configuring Multiple VLANs on cascaded switches can also affect Enhanced Stacking as the Master switch may not be able to detect member switches beyond the first cascaded switch.

Note
Port-based and Tagged VLAN configurations are restored when the user enables user-configured VLAN mode.

802.1Q-Compliant Multiple VLANs mode

802.1Q Multiple VLAN configuration is appropriate when the device connected to the uplink port is 802.1Q compatible, meaning that the device can handle tagged packets.

When 802.1Q Multiple VLANs mode is selected, the AT-S39 software configures all ports on that switch as Client VLANs except for one user-specified port that is designated as an Uplink VLAN (also referred to as management VLAN). Each Client VLAN on the switch is configured with one untagged port and one tagged port, a user-specified uplink port.

Upon selecting the 802.1Q-compliant VLAN mode, you are asked to specify the Uplink VLAN port. After specifying this port, all the ports on the switch are automatically configured.

For example, if your switch supports 26 ports and you selected 802.1Q-compliant VLAN mode , you would be asked to specify the Uplink VLAN port. If you selected 15, the VLANs would be configured as shown in the Table 8 example.

Note
In 802.1Q Multiple VLANs mode, any device connected to the uplink port must be 802.1Q-compliant.

Note
Procedures for configuring multiple VLANs can be found in **Multiple VLAN Configuration** on page 156.

Table 8 802.1Q-Compliant Multiple VLAN Example

VLAN Name	VID	Untagged Port	Tagged Port
Client_VLAN_1	1	1	15
Client_VLAN_2	2	2	15
Client_VLAN_3	3	3	15

VLAN Name	VID	Untagged Port	Tagged Port
Client_VLAN_4	4	4	15
Client_VLAN_5	5	5	15
Client_VLAN_6	6	6	15
Client_VLAN_7	7	7	15
Client_VLAN_8	8	8	15
Client_VLAN_9	9	9	15
Client_VLAN_10	10	10	15
Client_VLAN_11	11	11	15
Client_VLAN_12	12	12	15
Client_VLAN_13	13	13	15
Client_VLAN_14	14	14	15
Uplink_VLAN	**15**	**15**	
Client_VLAN_16	16	16	15
Client_VLAN_17	17	17	15
Client_VLAN_18	18	18	15
Client_VLAN_19	19	19	15
Client_VLAN_20	20	20	15
Client_VLAN_21	21	21	15
Client_VLAN_22	22	22	15
Client_VLAN_23	23	23	15
Client_VLAN_24	24	24	15
Client_VLAN_25	25	25	15
Client_VLAN_26	26	26	15

For information on Management VLANs, go to **Uplink VLANs - Multiple VLANs Mode Management** on page 159.

Non-802.1Q Compliant Multiple VLANs

Non-802.1Q Multiple VLAN configuration is appropriate when the device connected to the uplink port is non-802.1Q compatible, meaning that the device cannot handle tagged packets.

When Non-802.1Q Multiple VLANs is selected, the AT-S39 software configures all ports on that switch as Client VLANs except for one user-specified port that is designated as an Uplink VLAN (also referred to as management VLAN).

Each Client VLAN on the switch is configured as an untagged port and the user-specified Uplink VLAN is also configured as an untagged port that specifies all Client VLAN ports as untagged members.

Designating untagged ports in more than one VLAN at a time is what makes this configuration non-802.1Q compliant.

Upon selecting the Non-802.1Q Multiple VLANs, you are asked to specify the Uplink VLAN port. After specifying this port, all of the ports on the switch are automatically configured.

For example, if your switch supports 26 ports and you selected Non-802.1Q Multiple VLANs , you would be asked to specify the Uplink VLAN port. If you selected 15, the VLANs would be configured as shown in the Table 9 example. In this example, ports 1 to14 and 16 to 26 are configured as untagged Client VLANs and port 15, the Uplink VLAN is configured as an untagged member that includes all Client VLAN ports as members.

Caution
The non-802.1Q-Compliant Multiple VLAN mode does not protect the switch from VLAN leakages. If the switch receives a packet on the uplink port containing a destination MAC address that is not in the MAC address table, the switch will broadcast the packet out all ports, except the uplink port. This means that all end nodes on the switch will receive the packet.

Note
Procedures for configuring multiple VLANs can be found in **Multiple VLAN Configuration** on page 156.

Table 9 Non-802.1Q Compliant Multiple VLANs Example

VLAN Name	VID	Untagged Port	Tagged Port
Client_VLAN_1	1	1,15	
Client_VLAN_2	2	2,15	

VLAN Name	VID	Untagged Port	Tagged Port
Client_VLAN_3	3	3,15	
Client_VLAN_4	4	4,15	
Client_VLAN_5	5	5,15	
Client_VLAN_6	6	6,15	
Client_VLAN_7	7	7,15	
Client_VLAN_8	8	8,15	
Client_VLAN_9	9	9,15	
Client_VLAN_10	10	10,15	
Client_VLAN_11	11	11,15	
Client_VLAN_12	12	12,15	
Client_VLAN_13	13	13,15	
Client_VLAN_14	14	14,15	
Uplink_VLAN	**15**	**ALL**	
Client_VLAN_16	16	16, 15	
Client_VLAN_17	17	17,15	
Client_VLAN_18	18	18,15	
Client_VLAN_19	19	19,15	
Client_VLAN_20	20	20,15	
Client_VLAN_21	21	21,15	
Client_VLAN_22	22	22,15	
Client_VLAN_23	23	23,15	
Client_VLAN_24	24	24,15	
Client_VLAN_25	25	25,15	
Client_VLAN_26	26	26,15	

For information on Management VLANs, go to **Uplink VLANs - Multiple VLANs Mode Management** on page 159.

Chapter 11
Configuring User-Created VLANs

This chapter contains procedures for creating, modifying, and deleting user-configured VLANs from a local or Telnet management session.

For overviews of user-configured port-based and tagged-base VLANs, refer to the previous chapter:

- **User-Configured VLANs** on page 121
- **Port-based VLAN Overview** on page 121
- **Tagged VLAN Overview** on page 127

To create port-based and tagged-base VLANs, the switch mode must be set to tagged. For instructions on setting the switch mode, please refer to **Setting the Switch Mode** on page 117.

This chapter contains the following sections:

- **Creating a New Port-based or Tagged VLAN** on page 138
- **Creating a Port-based VLAN Example** on page 142
- **Creating a Tagged VLAN Example** on page 143
- **Modifying a VLAN** on page 144
- **Displaying VLAN Information** on page 147
- **Deleting a VLAN** on page 148
- **Deleting All VLANs** on page 150
- **Displaying PVIDs and Priorities** on page 151
- **Enabling or Disabling Ingress Filtering** on page 152
- **Designating a Management VLAN** on page 154

Creating a New Port-based or Tagged VLAN

To create a new port-based or tagged VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.

   The VLAN Menu shown in Figure 36 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                    VLAN Menu


1 - VLANs Status ..............Enabled
2 - Ingress Filtering Status ....Enabled
3 - VLANs Mode ..................User Configured
4 - Management VLAN .............1 (Default_VLAN)
5 - Configure VLANs
6 - Configure COS Priorities
7 - Show VLANs
8 - Show PVIDs & Priorities

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 36 VLAN Menu

2. From the VLAN Menu, type **5** to select Configure VLANs. The Configure VLANs menu in Figure 37 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
             Login Privilege: Manager

                 Configure VLANs


1 - Create VLAN
2 - Modify VLAN
3 - Delete VLAN
4 - Clear All Vlans

S - Save Configuration changes
R - Return to Previous Menu
```

Figure 37 Configure VLANs Menu

3. From the Configure VLANs menu, type **1** to select Create VLAN.

   The Create VLAN menu in Figure 38 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                   Create VLAN


1 - VLAN Name ............
2 - VLAN ID (VID) ........ 2
3 - Tagged Ports .........
4 - Untagged Ports .......
5 - Mirror Port ....... None

C - Create VLAN
R - Return to Previous Menu

Enter your selection?
```

Figure 38 Create VLAN Menu

4. Type **1** to select VLAN Name and enter a name for the new VLAN. The VLAN name can be from one to fifteen characters in length. The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!).

If the VLAN will be unique in your network, then the name should be unique as well. If the VLAN will be part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected. Using this type of naming convention, makes multiple switches in a network easier to maintain, administer, and troubleshoot.

Note
A VLAN must be assigned a name.

5. Type **2** to select VLAN ID (VID) and enter a VID value for the new VLAN. The permitted range of the VID value is 2 to 4094.

   The management software will use the next available VID number on the switch as the default value. If this VLAN will be unique in your network, then its VID must also be unique. If this VLAN will be part of a larger VLAN that spans multiple switches, than the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that will span three switches, you must assign the Sales VLAN on each switch the same VID value.

   Note
   A VLAN must have a VID.

6. If the VLAN will contain tagged ports, type **3** to select Tagged Ports and specify the ports. If this VLAN will not contain any tagged ports, leave this field empty.

   You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

7. Type **4** to select Untagged Ports and specify the ports on the switch to function as untagged ports in the VLAN. If this VLAN will not contain any untagged ports, leave this field empty.

   You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

8. If you want all received traffic on the ports of the VLAN to be mirrored to another port on the switch, type **5** to select Mirroring Port and enter a port number when prompted.

   This feature is useful when troubleshooting a VLAN. By placing a packet sniffer on the mirroring port, you can analyze the VLAN traffic.

As mentioned in **Port Mirroring Overview** on page 93, the following guidelines should be observed when creating a port mirror:

- ❑ You can mirror from one to 23 ports on a switch at a time.

However, the more ports you mirror, the less likely the mirroring port will be able to handle all the traffic. For example, if you mirror the traffic of six heavily active ports, the mirror port is likely to drop packets, meaning that it will not provide an accurate mirror of the traffic of the other six ports.

- ❑ The ports to be mirrored and the mirroring port must be located on the same switch.
- ❑ The ports to be mirrored and the mirroring port must be operating at the same speed. For example, you cannot use a 10/100 Mbps port to mirror traffic on a 1000 Mbps GBIC port.

Note
In most cases, this parameter should be left with its default value of 0. A value of 0 means that the VLAN traffic will not be mirrored. For more information on port mirroring, refer to **Port Mirroring Overview** on page 93.

9. Type **C** to select Create VLAN.

   If the switch is successful in creating the new VLAN, you will see the following message:

   ```
   SUCCESS - Press any key to continue.
   ```

10. Press any key.

    The Configure VLANS menu in Figure 37 is displayed.

11. Type **S** to select Save Configuration Changes.
12. Press Esc or type **R** to return to the Configure VLANS menu. If you would like to verify that the VLAN was created correctly, complete steps 13 through 14. Otherwise, you can repeat this procedure to create additional VLANs.
13. type 7 to select Show VLANs.
14. Check to see that the VLAN was created correctly and that it contains the appropriate ports.

Note
When you create a new VLAN, ports designated as untagged ports of the new VLAN are automatically removed from their current untagged VLAN assignment. For example, if you are creating a new VLAN on a switch that contains only the Default_VLAN, the ports that you specify as untagged ports of the new VLAN are automatically removed from the Default_VLAN.

Tagged ports are not removed from any current VLAN assignments because tagged ports can belong to more than one VLAN at a time.

Creating a Port-based VLAN Example

The following procedure creates the Sales VLAN illustrated in Figure 33 on page 124. This VLAN will be assigned a VID of 2 and will consist of four untagged ports, Ports 1 to 4. The VLAN will not contain any tagged ports. The VLAN traffic will not be mirrored on another port.

To create the example Sales VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANS.
3. From the Configure VLANS menu, type **1** to select Create VLAN.
4. Type **1** to select VLAN Name and enter “Sales”. Press Return.
5. Type **2** to select VLAN ID (VID) and enter “2”. This is the VID value for the new VLAN. Press Return.
6. Type **4** to select Untagged Ports and enter “1-4”. These are the untagged ports of the VLAN. Press Return.
7. Type **C** to select Create VLAN.
8. After the switch displays the prompt notifying you that it created the VLAN, press any key.
9. Type **S** to select Save Configuration Changes.

   The new Sales VLAN has been created.

Creating a Tagged VLAN Example

The following procedure creates the Engineering VLAN in the top switch illustrated in Figure 35 on page 130. This VLAN will be assigned a VID of 3. It will consist of four untagged ports, Ports 9, 10, 11, and 20, and two tagged ports, Ports 8 and 16. The VLAN traffic will not be mirrored on another port.

To create the example Engineering VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANs.
3. From the Configure VLANs menu, type **1** to select Create VLAN.
4. Type **1** to select VLAN Name and enter “Engineering”. Press Return.
5. Type **2** to select VLAN ID (VID) and enter “3”. This is the VID value for the new VLAN. Press Return.
6. Type **3** to select Tagged Ports and enter “8,16”. These are the tagged ports of the VLAN. Press Return.
7. Type **4** to select Untagged Ports and enter “9,10,11, 20”. These are the untagged ports of the VLAN. Press Return.
8. Type **C** to select Create VLAN.
9. After the switch displays the prompt notifying you that it created the VLAN, press any key.
10. Type **S** to select Save Configuration Changes.

    The new Engineering VLAN has been created.

Modifying a VLAN

Note
To modify a VLAN, you must know the VLAN VID. To view VLAN VIDs, refer to the procedure **Displaying VLAN Information** on page 147.

To modify a VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANS.
3. From the Configure VLANS menu, type **2** to select Modify a VLAN.

   The Modify a VLAN menu in Figure 39 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                  Modify VLAN


1 - VLAN ID (VID) ........

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 39 Modifying a VLAN Menu

4. Type **1** to select VLAN ID (VID).

   The following prompt is displayed:

   ```
   Enter new value -> [1 to 4096] ->
   ```

5. Enter the VID of the VLAN you want to modify. Press Return.

   The Modify a VLAN menu for the selected VLAN is displayed. This menu contains all relevant information about the VLAN.

6. Change the VLAN's information as desired.

   The menu selections are described below:

   1 - VLAN Name
   Use this selection to change a VLANs name. The name can be from one to fifteen characters in length. The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name can contain spaces, but not special characters, such as asterisks (*) or exclamation points (!).

When changing a VLAN's name, observe the following guidelines:

- A VLAN's new name cannot be the same as the name of another VLAN on the same switch. For example, if the switch already contains a VLAN called Sales, you cannot change an existing VLAN's name to Sales.
- You cannot change the name of the Default_VLAN.

Note
A VLAN must be assigned a name.

2 - VLAN ID (VID)
This is the VLAN's VID value. You cannot change this value.

3 - Tagged Ports
Use this selection to add or remove tagged ports from the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

When adding or removing tagged ports, observe the following guidelines:

- To add or remove tagged ports, enter the new list of tagged ports for the VLAN. For example, if the VLAN currently contains tagged port 4 and you wanted to add port 7, you would enter "4,7".
- If the VLAN will not contain any tagged ports, leave this field empty.
- If the VLAN contains tagged ports and you want to remove them all, enter a 0 (zero) for this value.

4 - Untagged Ports
Use this selection to add or remove untagged ports from the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

When adding or removing untagged ports, observe the following guidelines:

- To add or remove untagged ports, enter the new list of untagged ports for the VLAN. For example, if the VLAN currently contains untagged ports 15 through 19 and you want to add ports 4 through 9, you would enter "4-9,15-19".
- If the VLAN does not contain untagged ports, leave this field empty.

- ❑ To remove all untagged ports from a VLAN, enter a 0 (zero) for this value.
- ❑ You cannot remove untagged ports directly from the Default_VLAN. Instead, you remove an untagged port from the Default_VLAN by assigning the port as an untagged port to another VLAN.

An untagged port removed from a VLAN is automatically returned to the Default_VLAN as an untagged port.

5 - Mirroring Port
Use this option to direct all received traffic on the ports of the VLAN to a mirror port on the switch. This feature is useful when troubleshooting a VLAN. By placing a packet sniffer on the mirroring port, you can analyze the VLAN traffic.

Note
In most cases, this parameter should be left with its default value of 0. A value of 0 means that the VLAN traffic will not be mirrored. For more information on port mirroring, refer to **Port Mirroring Overview** on page 93.

7. After making the desired changes, type **M** to select Modify VLAN.

   A confirmation prompt is displayed.

8. Press any key.
9. Type **S** to select Save Configuration Changes.

   The VLAN has been modified.

10. Repeat this procedure starting with Step 4 to modify other VLANs.

Displaying VLAN Information

To view the name, VID number, and member ports of all the VLANs on a switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **7** to select Show VLANs.

   The Show VLANs menu is displayed (see Figure 40).

```
            Allied Telesyn Ethernet Switch AT-8024
                          Show VLANs
Login Privilege: Manager
VID          VLAN Name      Mirror  Untagged (U) / Tagged (T)
-----------------------------------------------------------------


1            Default_VLAN           U: 20-24
                                    T: 7,9
2            Sales                  U: 1-7
                                    T: 9
3            Production             U: 8-19
                                    T: 7


N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 40 Show VLANs Menu - User Configured

Deleting a VLAN

Note
To perform this procedure, you must know the VID of the VLAN that you want to delete. To view a VLAN's VID, refer to the procedure **Displaying VLAN Information** on page 147.

To delete a VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANS.
3. From the Configure VLANS menu, type **3** to select Delete VLAN.

   The Delete a VLAN menu in Figure 41 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                 Delete a VLAN

1 - VLAN ID (VID) ........

R - Return to Previous Menu

Enter your selection?
```

Figure 41 Delete a VLAN Menu

4. Type **1** to select VLAN ID (VID).

   The following prompt is displayed:

   ```
   Enter new value -> [2 to 4096] ->
   ```

5. Enter the VID of the VLAN you want to delete and press Return.

Note
You cannot delete the Default_VLAN, which has a VID of 1.

The specifications of the selected VLAN are displayed. Use this menu to confirm that you are deleting the correct VLAN.

6. Type **D** to delete the VLAN or **R** to cancel the procedure.

   The following confirmation prompt is displayed:

   ```
   Are you sure you want to delete this VLAN [Yes/No] ->
   ```

7. Type **Y** to delete the VLAN or **N** to cancel the procedure. Press Return.

   A confirmation message is displayed:

8. Press any key.
9. Type **S** to select Save Configuration Changes.

   The VLAN has been deleted. All untagged ports in the deleted VLAN are returned to the Default_VLAN as untagged ports.

10. Repeat this procedure starting with Step 4 to delete other VLANs.

Deleting All VLANs

This section contains the procedure for deleting all VLANs, except the Default_VLAN, on a switch.

Note
To delete selected VLANs, perform the procedure **Deleting a VLAN** on page 148.

To delete all VLANs on a switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **5** to select Configure VLANS.
3. From the Configure VLANS menu, type **4** to select Clear All VLANs.

   The following confirmation message is displayed:

   ```
   This operation deletes ALL user created VLANs!
   Do you want to continue [Yes/No] ->
   ```

4. Type **Y** to delete all VLANs or **N** to cancel the procedure. Press Return.

   A confirmation message is displayed.

5. Press any key.
6. Type **S** to select Save Configuration Changes.

   All VLANs are deleted and their tagged and untagged ports are returned to the Default_VLAN as untagged ports.

Displaying PVIDs and Priorities

The following procedure displays a window that lists the PVIDs for all the ports on the switch. The window also contains the current priority queue settings for each port. To display the PVID settings on the switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **8** to select Show PVIDs & Priorities.

   The Show PVIDs & Priorities window is displayed. An example of the window is shown in Figure 42.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
             Show PVIDs & Priorities


Port  PVID      Priority   Override Priority
-----------------------------------------------

01     1          0             No
02     1          0             No
03     1          0             No
04     1          0             No
05     1          0             No
06     1          0             No
07     1          0             No

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 42 Show PVIDs and Priorities Window

The PVID column displays the current PVID value for each switch port.

Note
The Priority and Override Priority columns relate to the switch's Class of Service feature. For information, refer to **Chapter 14**, **Class of Service** on page 174.

Enabling or Disabling Ingress Filtering

There are certain rules that a switch follows as it receives and forwards an Ethernet frame. There are rules for frames as they enter a port (called *ingress rules*) and rules for when a frame is transmitted out a port (called *egress rules*). A switch will not accept and forward a frame unless the frame passes the ingress and egress rules.

There are quite a few ingress and egress rules for Fast Ethernet switches. Fortunately, this discussion need only review the rules as they apply to tagged frames, because ingress filtering does not apply to untagged frames, nor to any frames, tagged or untagged, when the switch is operating in the Basic Mode.

First, just as a reminder, a tagged frame is an Ethernet frame that contains a tagged header. The header contains the VID of the VLAN to which the frame originated. For further information, refer to **User-Configured VLANs** on page 121.

Let's first examine how the ingress rules are applied to tagged frames when ingress filtering is enabled. What the switch does is it examines the tagged header of each tagged frame that enters a port and determines whether the tagged frame and the port that received the frame are members of the same VLAN. If they belong to the same VLAN, the port accepts the frame. If they belong to different VLANs, the port discards the frame.

Here is an example. Assume that a tagged frame with a VID of 4 is received on a tagged port that is a member of a VLAN also with a VID of 4. In this case, the port accepts the frame, because both the frame and the port belong to the same VLAN. If the frame and port had belonged to different VLANs, the frame is discarded.

So how do the ingress rules apply when ingress filtering is disabled? First, any tagged frame is accepted on any port on the switch. It does not matter whether the frame and the port belong to the same or different VLANs.

Once the tagged frame is received, the switch examines the tagged header and determines if the VID in the header corresponds to any VLANs on the switch. If there isn't a corresponding VLAN, the switch discards the frame. If there is, the switch transmits the frame out the port to the destination node, assuming that the destination node's MAC address is in the MAC address table, or floods the port to all ports on the VLAN if the MAC address is not in the table.

There is one other thing that should be mentioned about ingress filtering and tagged packets, and that is the priority tag. Each tagged frame has a priority tag in it that instructs the switch as to the importance of the frame. Frames with a high priority are handled ahead of frames with a low priority.

Activating or deactivating ingress filtering has no effect on the switch's handling of priority tags. A switch will always examine a priority tag in a tagged frame, regardless of the status of ingress filtering.

In most cases, you will probably want to leave ingress filtering activated on the switch, which is the default. You can enable or disable ingress filtering on a per switch basis. You cannot set this per port.

To enable or disable ingress filtering, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **2** to select Ingress Filtering Status. Current status for this functionality (enabled or disabled) is displayed next to this feature selection.The following prompt is displayed:

   ```
   Enter Ingress Filtering Status (E-Enable, D-Disable)
   ->
   ```

3. Type **E** to activate ingress filtering or **D** to disable ingress filtering on the switch.
4. Type **S** to select Save Configuration Changes.

   A change to the status of ingress filtering is immediately activated on the switch.

Designating a Management VLAN

To remotely manage an AT-8300 Series Switch, there must exist a communications path through which the management station and the switch to be managed can communicate. If the management station is connected directly to a port on the switch, either through a tagged or untagged port, then the communications path automatically exists and you can fully manage the switch.

However, if there is one or more intermediate Ethernet switches between the management station and the switch to be managed, then it may be necessary for you to manually create a communications path. This is accomplished by specifying a management VLAN.

The management VLAN is the VLAN through which a remote management station communicates with a managed switch. By default, the management VLAN is the Default_VLAN. If you do not create any new VLANs in your network and if your AT-8000 Series Switches are interconnected with either tagged or untagged ports, then you will not need to create or specify a new management VLAN.

However, if you do create additional VLANs in your network, then you might need to change the management VLAN. Below are several rules to observe when using this feature:

- ❑ The management VLAN must exist on each AT-8000 Series switch that you want to manage.
- ❑ Using the procedure on the following page, you must specify the management VLAN in the AT-S39 software on each slave and master switch of an enhanced stack.
- ❑ The uplink and downlink ports on each switch that are functioning as the tagged or untagged data links between the switches must be either tagged or untagged members of the management VLAN.
- ❑ The port on the switch to which the management station is connected must be a member of the management VLAN. (This rule does not apply when managing the switch locally through the RS232 Terminal Port.)

Here is an example. Let's assume that you have an enhanced stack of seven AT-S39 Series switches with one master switch. If the uplink and downlink ports between the various switches are members of the Default_VLAN and if the management station is connected to a port of the Default_VLAN, you will be able to manage all the switches since the Default_VLAN is by default the management VLAN.

Now let's assume that you have decided to create a VLAN called NMS with a VID of 24 for the sole purpose of remote network management. For this, you would need to create the NMS VLAN on each AT-8000 Series switch that you want to manage remotely, being sure to assign each NMS VLAN the VID of 24. Then you would need to be sure that the uplink and downlink ports connecting the switches together are either tagged or untagged members of the NMS VLAN. You would also need to specify the NMS VLAN as the management VLAN on each switch using the management software. Finally, you must be sure to connect your management station to a port on a switch that is a tagged or untagged member of the management VLAN.

To specify the management VLAN in the AT-S39 software, do the following:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **4** to select Management VLAN.

   The following prompt is displayed:

   ```
   Enter Management VLAN ID [1 to 4094] ->
   ```

3. Specify the VID of the VLAN that is to function as the management VLAN. This VLAN must already exist on the switch.

   The following prompt is displayed:

   ```
   SUCCESS - Press any key to continue ...
   ```

4. Press any key.
5. Type **S** to select Save Configuration Changes.

Chapter 12
Multiple VLAN Configuration

This chapter contains explains how to select a multiple VLAN mode. For an overview on multiple VLANs mode, refer to the following sections **Multiple VLAN Mode Overview** on page 132.

To select a multiple VLAN configuration, the switch mode of the switch must be set to tagged. For instructions on setting the switch mode, please refer to **Setting the Switch Mode** on page 117.

This chapter contains the following sections:

- **Preserving User-Configured VLAN Definitions** on page 157
- **Activating or Deactivating the Multiple VLAN Mode** on page 158
- **Uplink VLANs - Multiple VLANs Mode Management** on page 159
- **Displaying VLAN Information** on page 160

Preserving User-Configured VLAN Definitions

When the VLAN mode is set to either of the Multiple VLAN mode, user-configured VLAN definitions cannot be created or modified. However, the software preserves user-configured VLANs that were configured before multiple VLAN mode was enabled. When the user switches back to user-configured VLANs mode, the software automatically enables the user-configured VLANs with the pre-existing configuration.

Activating or Deactivating the Multiple VLAN Mode

The following procedure explains how to enable or disable multiple VLANs mode on an AT-8000 Series Switch.

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **3** to select VLANs Mode. Current status for this functionality (enabled or disabled) is displayed next to this feature selection. The following prompt is displayed:

   ```
   Enter VLAN Mode (U-UserConfig, M-Multiple, Q-802.1Q
   Multiple VLANs) ->
   ```

3. Type **M** to enable Non-802.1Q compliant multiple VLANs , **Q** to enable Q-802.1Q Multiple VLANs, or **U** to create your own port-based and tagged VLANs. The following prompt is displayed:

   ```
   Enter Uplink VLAN Port number ->  [1 to 26] ->
   ```

4. Enter the Uplink VLAN port number. The following confirmation is displayed:

   ```
   SUCCESS - VLAN Mode set to Multiple VLANs mode
   ```

Note
For additional information on Multiple VLAN mode, refer to **Multiple VLAN Mode Overview** on page 132.

Uplink VLANs - Multiple VLANs Mode Management

An overview of management VLANs is provided in the previous chapter (**Designating a Management VLAN** on page 154). Although both multiple VLAN modes support remote management of the switch via a management VLAN, the management VLAN would be designated to the Uplink VLAN port and the user would not be allowed to modify it. If you are in multiple VLAN mode and you select the Management VLAN parameter in the VLAN menu, the following message is displayed:

```
Management VLAN can not be changed in Multiple VLANs
mode
```

Displaying VLAN Information

To view the name, VID number, and member ports of all the VLANs on a switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **7** to select Show VLANs.

   The Show VLANs window is displayed. An example of the window is shown in Figure 43.

```
              Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                              Show VLANs


VID     VLAN Name             Untagged Port(s)     Tagged Port(s)
------------------------------------------------------------------
------
1       Client_VLAN_1           1, 15                    ---
2       Client_VLAN_2           2, 15                    ---
3       Client_VLAN_3           3, 15                    ---
4       Client_VLAN_4           4, 15                    ---
5       Client_VLAN_5           5, 15                    ---
6       Client_VLAN_6           6, 15                    ---
7       Client_VLAN_7           7, 15                    ---
8       Client_VLAN_8           8, 15                    ---

N - Next Page
U - Update Display
R - Return to Previous Menu
```

Figure 43 Show VLANs Window -Multiple VLAN

Chapter 13
MAC Address Table

The chapter contains the procedures for viewing the static and dynamic MAC address table.

This chapter contains the following sections:

- **MAC Address Overview** on page 162
- **Displaying MAC Addresses** on page 164
- **Viewing MAC Addresses by Port** on page 167
- **Identifying a Port Number by MAC Address** on page 168
- **Viewing the MAC Addresses of a VLAN** on page 169
- **Deleting All Dynamic MAC Addresses** on page 170
- **Adding Static and Multicast MAC Addresses** on page 171
- **Deleting MAC Addresses** on page 172
- **Changing the Aging Time** on page 173

MAC Address Overview

Every hardware device that you connect to your network has a unique MAC address associated with it. A MAC address is assigned to a device by the device's manufacturer. For example, every network interface card that you use to connect your computers to your network has a MAC address assigned to it by the adapter's manufacturer.

The AT-8000 Series switch contains a 4 kilobyte MAC address table. The switch uses the table to store the MAC addresses of the network nodes connected to its ports, along with the port number on which each address was learned.

The switch learns the MAC addresses of the end nodes by examining the source address of each packet received on a port. It adds the address and port on which the packet was received to the MAC table if the address has not already been entered in the table. The result is a table that contains all the MAC addresses of the devices that are connected to the switch's ports, and the port number where each address was learned.

When the switch receives a packet, it also examines the destination address and, by referring to its MAC address table, determines the port where the destination node is connected. It then forwards the packet to the appropriate port and on to the end node. This increases network bandwidth by limiting each frame to the appropriate port when the intended end node is located, freeing the other switch ports for receiving and transmitting data.

If the switch receives a packet with a destination address that is not in the MAC address table, it floods the packet to all the ports on the switch. If the ports have been grouped into virtual LANs, the switch floods the packet only to those ports which belong to the same VLAN as the port on which the packet was received. This prevents packets from being forwarded onto inappropriate LAN segments and increases network security. When the destination node responds, the switch adds its MAC address and port number to the table.

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. Since both the source node and the destination node for the packet are located on the same port on the switch, there is no reason for the switch to forward the packet. This too increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

The type of MAC address described above is referred to as a *dynamic MAC address*. Dynamic MAC addresses are addresses that the switch learns by examining the source MAC addresses of the frames received on the ports.

Dynamic MAC addresses are not stored indefinitely in the MAC address table. The switch deletes a dynamic MAC address from the table if it does not receive any frames from the node over a specified period of time. The switch assumes that the node with that MAC address is no longer active and that its MAC address can be purged from the table. This prevents the MAC address table from becoming filled with addresses of nodes that are no longer active.

The period of time that the switch waits before purging an inactive dynamic MAC address is called the *aging timer*. This value is adjustable on the AT-8000 Series switch. The default value is 300 seconds (5 minutes). For instructions on changing the aging timer, refer to **Changing the Aging Time** on page 173.

The MAC address table can also store *static MAC addresses*. A static MAC address, once entered in the table, remains in the table indefinitely and is never deleted, even when the end node is inactive.

You might need to enter static MAC addresses of end nodes the switch will not learn in its normal dynamic learning process, or if you want a MAC address to remain permanently in the table, even when the end node is inactive.

Displaying MAC Addresses

The management software has two menu selections for displaying the MAC addresses of a switch. One selection displays the static, dynamic, and multicast MAC addresses while the other displays just the static and multicast addresses, but no dynamic addresses.

To display the MAC address table, perform the following procedure:

1. From the Main Menu, type **6** to select MAC Address Tables.

   The MAC Address Table menu in Figure 44 is displayed.

```
      Allied Telesyn AT-8024 Ethernet Switch
Login Privilege: Manager
                MAC Address Tables


1 - Show all MAC Addresses
2 - Add static MAC Address
3 - Delete MAC Address
4 - Delete all dynamic MAC Addresses
5 - Show all static MAC addresses
6 - View MAC addresses by Port
7 - View the port of MAC address
8 - View MAC addresses by VLAN ID
9 - View IP Multicast MAC Addresses
A - View MAC addresses on base ports

R - Return to Previous Menu

Enter your selection?
```

Figure 44 MAC Address Table Menu

2. To display both static and dynamic MAC addresses, type **1** to select Show All MAC Addresses or **A** to select View MAC Addresses on Base Ports. The second selection is useful if you are managing an AT-8000 Series switch with GBIC or expansion modules installed, and you want to view the MAC addresses only on Ports 1 to 24.
3. To display only static MAC addresses, type **5** to select Show All Static MAC Addresses.

The management software displays the MAC addresses. Figure 45 is an example of the Show All MAC Addresses window, which displays both static and dynamic MAC addresses. The static MAC address window is exactly the same, except for the title and the fact that it displays only static MAC addresses.

```
                    Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                             Show All MAC Addresses


MAC               Port PMAP     CPU MIR  EMP  VlanID Type
------------------------------------------------------------------------
01:80:C1:00:02:01 0    00000000 Yes Yes  Yes  0      Static (fixed, non-aging)
00:a0:d2:18:1a:c8 1    00000000 No  No   No   1      Dynamic
00:a0:c4:16:3b:80 2    00000000 No  No   No   1      Dynamic
00:a0:12:c2:10:c6 3    00000000 No  No   No   1      Dynamic
00:a0:c2:09:10:d8 4    00000000 No  No   No   1      Dynamic
00:a0:33:43:a1:87 5    00000000 No  No   No   1      Dynamic
00:a0:12:a7:14:68 6    00000000 No  No   No   1      Dynamic
00:a0:d2:22:15:10 7    00000000 No  No   No   1      Dynamic
00:a0:d4:18:a6:89 8    00000000 No  No   No   1      Dynamic

U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 45 Show All MAC Addresses Window

The information is for viewing purposes only. The columns in the window are defined below.

MAC
The MAC address of the node connected to the switch.

Port
The port on the switch where the MAC address was learned.

PMAP
The ports on the switch that are members of a multicast group. This column is useful in determining which ports belong to different multicast groups. (The abbreviation PMAP is derived from "port mapping.")

Each "0" is a hexadecimal value for the binary value "0000". Each binary "0" represents a port on the switch. A binary "0" means that the port is not a member of a multicast group while a "1" means that it is.

The port numbering scheme is from right to left. As an example, assume that ports 1 through 4 on the switch were members of the same multicast group. This would be represented in the column as follows: “0000000F”. Another example is “000020F. This example would indicate that ports 1 to 4 and port 10 on the switch were members of the same multicast group.

CPU
This feature is not supported.

MIR
Indicates whether the traffic on the port is being mirrored. Yes means the traffic is being mirrored while No indicates that it is not.

EMP
Indicates whether multicast packets are being forwarded by ports in the blocking state. This feature is not supported at this time. This column will indicate “No” for all multicast addresses, except for the switch’s MAC address. Multicast packets are forwarded only by ports in the forwarding state.

VLANID
The VID of the VLAN to which the port is an untagged member.

Type
The MAC address type. The type can be either static or dynamic.

Viewing MAC Addresses by Port

This section contains the procedure for viewing the dynamic MAC addresses that have been learned on a particular port. You can also use this procedure to view any static MAC addresses that have been assigned to a port.

1. From the Main Menu, type **6** to select MAC Address Table.
2. From the MAC Address Tables menu, type **6** to select View MAC Addresses by Port Menu.

   The following prompt is displayed:

   ```
   Please enter port number -> [1 to 26] ->
   ```
3. Enter the number of the port whose static and dynamic MAC addresses you want to view and press Return.

   A window is displayed with the MAC addresses of the end nodes on the port. The columns in the window and the definitions of the columns are the same as for the Show All MAC Addresses window on page 165.

   The information in this window is for viewing purposes only.

Identifying a Port Number by MAC Address

In some situations, you might want to know which port a particular MAC address was learned. You could display the MAC address table and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding the address could prove difficult.

The procedure in this section offers an easier way. You can specify the MAC address and let the management software automatically locate the port on the switch where the device is connected.

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **7** to select View the Port of MAC Address.

   The following prompt is displayed:

   ```
   Please enter MAC address:
   ```
3. Enter the MAC address of the node in the following format and press Return:

   ```
   XXXXXX XXXXXX
   ```

   The management software displays a prompt containing the port number on the switch to which the node is connected, if the address was learned dynamically, or to which the address was assigned, for a static address.

Viewing the MAC Addresses of a VLAN

The procedure in this section can be useful if you created VLANs on the switch and want to view the MAC addresses of the nodes of a particular VLAN. (This procedure is not of much value if the switch contains only the Default_VLAN, in which case displaying the entire MAC address table, as explained earlier in this chapter, produces the same result.)

Note
To perform this procedure, you need to know the VID number of the VLAN whose MAC addresses you want to view. To obtain a VLAN's VID, refer to **Displaying VLAN Information** on page 147.

To view the MAC addresses of a VLAN on the switch, perform the following procedure.

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **8** to select View MAC Addresses by VLAN ID Menu.

   The following prompt is displayed:

   ```
   Please enter a VLAN ID: [1 to 4095] ->
   ```
3. Enter the VID of the desired VLAN and press Return.

   The management software displays a window with a list of the MAC addresses of the nodes in the VLAN. For an example of the window and for definitions of the columns, refer to the Show All MAC Addresses window on page 165.

Deleting All Dynamic MAC Addresses

The management software allows you to purge the MAC address table of all dynamic MAC addresses. Once the table has been purged, the switch immediately begins to relearn the MAC addresses as frames are received on the ports.

> **Note**
> This procedure does not delete static MAC addresses.

To delete all dynamic MAC addresses from the MAC address table, perform the following procedure.

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **4** to select Delete All Dynamic MAC Addresses.

   A following prompt is displayed:

   ```
   All learned MAC (non-static) addresses will be
   deleted.
   Do you want to continue? [Yes/No] ->
   ```

3. Type **Y** for yes to delete the dynamic MAC addresses or **N** for no to cancel the procedure.

   If you type **Y** for yes, the dynamic MAC addresses are deleted from the MAC address table. The switch immediately begins to relearn the addresses and to add them to the table.

Adding Static and Multicast MAC Addresses

This section contains the procedure for adding static and multicast addresses to the switch. You can assign up to 255 static MAC addresses per port on an AT-8000 Series switch.

To add a static or multicast address to the MAC address table, perform the following procedure:

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **2** to select Add Static MAC Address.

   The following prompt is displayed:

   ```
   Please enter a MAC address ->
   ```
3. Enter the static MAC address in the following format:

   ```
   XXXXXX XXXXXX
   ```

   Once you have specified the MAC address, the following prompt is displayed:

   ```
   Please enter a port number: [1 to 24] ->
   ```
4. Enter the number of the port on the switch to which you want to assign the address.

   The management software adds the address to the MAC address table.
5. Repeat steps 2 to 4 to enter additional static or multicast MAC addresses.

Deleting MAC Addresses

The following procedure explains how to delete a static, dynamic, or multicast MAC address from the MAC address table.

To delete an address from the MAC address table, perform the following procedure:

1. From the Main Menu, type **6** to select MAC Address Tables.
2. From the MAC Address Tables menu, type **3** to select Delete MAC Address.

   The following prompt is displayed:

   ```
   Please enter a MAC address ->
   ```
3. Enter the MAC address to be deleted in the following format and press Return:

   ```
   XXXXXX XXXXXX
   ```

   The MAC address is deleted from the switch's MAC address table.

   Note
   You cannot delete a switch's MAC address, an STP BPDU MAC address, or a broadcast address.

4. Repeat the procedure to delete additional MAC addresses.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default setting for the aging time is 300 seconds (5 minutes).

To adjust the aging time, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Config Menu, type **1** to select MAC Aging Time.

   The following prompt is displayed:

   ```
   Enter your new value -> [1 to 1048575]
   ```
3. Enter a new value in seconds.

   The value should be an increment of 5 seconds, for example 410, 415, or 420. A value that is not an increment of 5 is rounded down to the next increment of 5. For example, the value 524 is rounded down to 520.

   The new value is immediately activated on the switch.

Chapter 14
Class of Service

This chapter contains the procedures for configuring the Class of Service (CoS) feature of the AT-S39 software. Sections in the chapter include:

- **Class of Service Overview** on page 175
- **Configuring CoS** on page 176

Class of Service Overview

The AT-8000 Series switch supports CoS as specified in the IEEE 802.1p and 802.1Q standards. CoS can be important in network environments where there are time-critical applications, such as voice transmission or video conferencing, that can be adversely affected by packet transfer delays.

Prior to CoS, network traffic was handled in a best-effort manner. File transfer delays did occur, but were mostly transparent to network users. But with the introduction of time-critical applications, packet transfer delays can prove problematic. For example, transfer delays of voice transmission can result in poor audio quality.

CoS was designed to address this problem. The 802.1p standard outlines eight levels of priority, 0 to 7, with 0 the lowest priority and 7 the highest.

The AT-8000 Series switch has two priority queues, low and high. When a tagged packet enters a switch port, the switch responds by placing the packet into one of the two queues according to following assignments:

IEEE 802.1p Priority Levels	AT-8000 Series Switch Queue
7	high
6	high
5	high
4	high
3	low
2	low
1	low
0	low

For example, a tagged packet with a priority tag of 6 is placed in the high priority queue, while a packet with a priority tag of 1 is placed in the low priority queue.

These priority-to-queue assignments can be overridden using the AT-S39 management software on a per port basis.

You can also use CoS to control which priority queue handles untagged frames that ingress a port. By default, untagged frames (i.e., frames without VLAN or priority level information) are automatically assigned to the low priority buffer. But you can configure CoS on a port so that all untagged frames received on the port are directed to the high priority queue.

Configuring CoS

To configure CoS for a port, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **3** to select Configure Port VLANS & Priorities.
3. Type **1** to select Configure Port VLANs & Priorities. The following prompt is displayed:

   ```
   Enter port number -> [1 to 24] ->
   ```

4. Enter the number of the port on the switch where you want to configure CoS. Press Return. The Port VLANS & Priorities menu in Figure 36 on page 138 is displayed.
5. Type **3** to select Priority (0 - 7). The following prompt is displayed:

   ```
   Enter new value -> [0 to 7]
   ```

6. If you want all tagged and untagged frames received on the port to go to the low priority queue, enter a value from 0 to 3. (It does not matter which value you enter so long as it's from 0 to 3.) If you want all frames received on the port to go to the high priority queue, enter a value from 4 to 7. (Again, it does not matter which number it is so long as it is from 4 to 7.)
7. If you are configuring a tagged port and you want the switch to ignore the priority tag in the tagged frames that ingress the port, type **4** to select Override Priority and type **Y**.

   All tagged frames will be directed to either the low or high priority queue as specified in Step 6.

   Note
   The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered.

   The default for this parameter is No, meaning that the priority level of tagged frames is determined by the priority level specified in the frame itself.
8. Type **C** to select Configure Port VLANS & Priorities.
9. Type **S** to select Save Configuration Changes.
10. Repeat this procedure to configure CoS on other ports on the switch.

    Note
    To view the priority queue assignment for each port and the override priority status, refer to **Displaying PVIDs and Priorities** on page 151.

Chapter 15
IGMP Snooping

This chapter explains how to activate and configure the Internet Group Management Protocol (IGMP) snooping feature on the switch. Sections in the chapter include:

- **IGMP Snooping Overview** on page 178
- **Activating IGMP Snooping** on page 180
- **Displaying a List of Host Nodes** on page 183
- **Displaying a List of Multicast Routers** on page 184

IGMP Snooping Overview

IGMP snooping is best explained by first defining IGMP. This protocol enables routers to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node wanting to become a member of a particular multicast group responds to a query by sending a *report*. A report indicates an end node's intention to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. Once a host node has been made a member of a multicast group, it must continue to periodically issue reports to remain a member.

Once the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets out the port. This improves network performance by restricting multicast packets only to router ports where host nodes are located.

There are two versions of IGMP, referred to as Version 1 and Version 2. One of the differences between the two versions is how a host node indicates that it no longer wants to be a member of a multicast group. In Version 1, it simply stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a *time-out value*, it assumes that the host node no longer wants to receive multicast frames, and removes it from the membership list of the multicast group.

In Version 2, a host node exits from a multicast group by sending a *leave request*. Once a router receives a leave request from a host node, it removes the node from appropriate membership list. The router will also stop sending out multicast packets out the port to which the node is connected if it determines there are no further host nodes on the port.

IGMP snooping enables the Fast Ethernet switch to monitor the flow of queries from a router and reports from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets only to those switch ports connected to host nodes.

Without IGMP snooping, a switch would have to flood multicast packets out all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact switch and network performance.

The AT-8000 Series switch supports both IGMP Version 1 and Version 2. The switch maintains its multicast groups through an adjustable time-out value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note
By default, IGMP snooping is disabled on the switch.

Activating IGMP Snooping

To activate or deactivate IGMP snooping on the switch and to configure IGMP snooping parameters, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **A** to select Advanced Configuration.
3. From the Advanced Configuration menu, type **1** to select IGMP Snooping Configuration.

   The IGMP Snooping Configuration menu in Figure 46 is displayed.

```
          Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                IGMP Snooping Configuration


1 - IGMP Snooping Status ......... Disabled
2 - Multicast Host Topology ...... Single-Host/Port (Edge)
3 - Host/Router Timeout Interval . 260 seconds
4 - Maximum Multicast Groups ..... 256
5 - Multicast Router Port(s) ..... Auto Detect
6 - View Multicast Hosts List
7 - View Multicast Router List

S - Save Configuration Changes
R - Return to Previous Men

Enter your selection:
```

Figure 46 IGMP Snooping Configuration Menu

The options in the menu are defined below:

1 - IGMP Snooping Status
Enables and disables IGMP snooping on the switch. After selecting this option, type **E** to enable or **D** to disable this feature.

2 - Multicast Host Topology
Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Single-Host/Port (Edge) and Multi-Host/Port (Intermediate).

The Single-Host/Port setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a

multicast group by sending a leave request or when the host node stops sending reports. The switch responds by immediately ceasing the transmission of further multicast packets out the port where the host node is connected.

The Multi-Host setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port will continue to receive the multicast packets. Only after all the host nodes connected to a switch port have transmitted leave requests (or have timed out) will the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Multi-Host Port (Intermediate) selection.

3 - Host/Router Timeout Interval
Specifies the time period in seconds after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

4 - Maximum Multicast Groups
Specifies the maximum number of multicast groups the switch will learn. The range is 1 to 2048 groups. The default is 256 multicast groups.

This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

5 - Multicast Router Port(s)
Specifies the port on the switch to which the multicast router is detected. You can let the switch determine this automatically by selecting Auto Detect, or you can specify the port yourself by entering a port number. To select Auto Detect, enter "0" (zero) for this parameter. You can specify more than one port.

Note
Selections 6 and 7 in the menu are discussed later in this chapter.

4. After making the desired changes, type **S** to select Save Configuration Changes.

   Your changes are activated immediately on the switch.

Displaying a List of Host Nodes

You can use the AT-S39 software to display a list of the multicast groups on a switch, as well as the host nodes. To display the list, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **A** to select Advanced Configuration.
3. From the Advanced Configuration menu, type **1** to select IGMP Snooping Configuration.

   The IGMP Snooping Configuration menu in Figure 46 is displayed.
4. From the IGMP Snooping Configuration menu, type **6** to select View Multicast Host List.

   The View Multicast Host List in Figure 47 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
           View Multicast Hosts List
=============================================
MulticastGroup  MemberPort  VLAN   Host IP
=============================================

U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 47 View Multicast Hosts List Window

The information in this window is for viewing purposes only. The columns are defined below:

Multicast Group
The multicast address of the group.

Membership Port
The port(s) on the switch to which one or more host nodes of the multicast group are connected.

VLAN
The VID of the VLAN in which the port is an untagged member.

Host IP
The IP address(es) of the host node(s) connected to the port.

Displaying a List of Multicast Routers

A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. You can use the AT-S39 software to display a list of the multicast routers that are connected to the switch.

To display a list of the multicast routers, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **A** to select Advanced Configuration.
3. From the Advanced Configuration menu, type **1** to select IGMP Snooping Configuration.

   The IGMP Snooping Configuration menu in Figure 46 is displayed.
4. From the IGMP Snooping Configuration menu, type **7** to select View Multicast Routers List.

   The View Multicast Router List in Figure 47 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
          View Multicast Routers List


=========================================
Port           VLAN          Router IP
=========================================

U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 48 View Multicast Routers List Window

The information in this window is for viewing purposes only. The columns are defined below:

Port
The port on the switch where the multicast router is connected.

VLAN
The VID of the VLAN in which the port is an untagged member.

Router IP
The IP address of the multicast router.

Chapter 16
Broadcast Storm Control

This chapter contains the procedures for configuring the Broadcast Storm Control feature of the AT-S39 management software. Sections in the chapter include:

- **Broadcast Storm Control Overview** on page 186
- **Configuring the Interval Timer** on page 188
- **Configuring the Maximum Broadcast Frame Count** on page 190

Broadcast Storm Control Overview

Most frames on an Ethernet network are unicast frames. A unicast frame is a frame that is sent to a single destination. That is, the node sending a unicast frame intends the frame for a particular node on the network. For example, when a node needs to send a file to a network server for storage, the node sends the file in unicast Ethernet frames containing the destination address of the server where the file is to be stored.

Broadcast frames are different. Broadcast frames are directed to all nodes on the network or all nodes within a particular virtual LAN. Broadcast packets can perform a variety of functions in an Ethernet network. For example, some network operating systems use broadcast frames to announce the presence of devices on the network.

The problem with broadcast frames is that too many of them traversing a network can impact network performance. The more bandwidth consumed by broadcast frames, the less available for unicast frames.

Should the performance of your network be impacted by heavy broadcast traffic, you can use the AT-S39 management software to limit the number of broadcast frames that are forwarded by the switch and so limit the number of broadcast frames on your network.

You accomplish this by specifying the maximum number of broadcast frames that you want the switch to forward within a specified time interval. Broadcast frames that exceed the maximum on a port during the time interval are not forwarded and are dropped by the switch.

In order to use this feature, you must set two values: the *interval timer* and the *maximum broadcast frame limit*.

The interval timer defines the time period used in counting the number of forwarded broadcast frames on a port. There are two interval timers. One timer is for ports operating at 10 Mbps or 100 Mbps. The second timer is for 1000 Mbps ports. The timer interval for 10 and 100 Mbps ports is measured in milliseconds. The timer interval for 1000 Mbps ports is measured in microseconds. A time interval setting applies to all ports operating at the corresponding speed on the switch.

The maximum broadcast frame limit specifies the maximum number of broadcast frames the switch will forward on a port during the specified timer interval. Broadcast frames received once the maximum has been exceeded are not forwarded by the port and are discarded. You can specify a different maximum for each port on the switch.

It is important to note that the maximum number applies to the egress port of a broadcast frame, not the ingress port. That is, any port on the switch will accept any number of broadcast frames. But a port will transmit out (forward) a broadcast frame only if it has not exceeded the maximum number of broadcast frames it can transmit.

Here's an example. Let's assume you set the timer interval for 10 and 100 Mbps ports to 100 milliseconds and the maximum broadcast frame limit for a particular 100 Mbps port on the switch to 200 broadcast frames. At these settings, the port will forward (transmit out) up to 200 broadcast frames every 100 milliseconds. If the maximum is exceeded during the specified time interval, the port discards any additional broadcast frames and does not forward them.

Note
The AT-S39 default setting is no Broadcast Storm Control on the switch.

Configuring the Interval Timer

To set the interval timer for the Broadcast Storm Control feature, perform the following procedure:

1. From the Main Menu, type **5** to select System Config Menu.
2. From the System Configuration Menu, type **A** to select Advanced Configuration.
3. From the Advanced Configuration Menu, type **2** to select Broadcast Timers Setup.

   The Broadcast Storm Control menu in Figure 49 is displayed.

```
      Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
              Broadcast Storm Control


1 - Timer for 10/100 MB ports ..... 10 milli sec
2 - Timer for 1000 MB ports ....... 100 micro sec

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 49 Broadcast Storm Control Menu

4. Type **1** or **2** and enter a value when prompted.

   The interval timer for 10 Mbps and 100 Mbps ports is in milliseconds and has a range of 10 to 120 milliseconds. The value should be entered in increments of 10.

   The interval timer for 1000 Mbps ports is in microseconds and has a range of 100 to 120000 microseconds. The value should be entered in increments of 100.

   A value for an interval timer applies to all ports operating at the corresponding speed.

   Note
   The 1000 Mbps speed applies only to GBIC modules in AT-8024GB switches and expansion modules in an AT-8016F Series, AT-8012M, and AT-8024M switch.

5. Once you have set the desired timer intervals, type **S** to select Save Configuration Changes.

   Your changes are immediately activated on the switch.

6. Go to the next procedure and specify the maximum number of broadcast frames the ports on the switch can receive.

Configuring the Maximum Broadcast Frame Count

To specify the maximum number of broadcast frames a port on the switch can receive and forward, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **1** to select Port Configuration.

   The following prompt is displayed:

```
Enter Ports List ->
```

3. Enter the port(s)that you want to configure and press Return.

   The Port Configuration menu is shown in Figure 14 on page 69.

4. Type **B** to select Broadcast Control.

   The following prompt is displayed:

```
Enter Max. Broadcasts (0 -> No limit) :
[0 to 1023] - >
```

5. Specify the maximum number of broadcast frames the port can receive during the timer interval. Press Return.

   For example, assume that you are specifying the maximum broadcast frame count for a port operating at 100 Mbps, and you specified a 10 millisecond interval timer for 100 Mbps ports. If you entered a value of 200 at the prompt, the switch will transmit a maximum of 200 broadcast frames on the port every 10 milliseconds. If more than 200 broadcast frames are transmitted by the port during the time interval, all broadcast frames over 200 are discarded by the port and are not forwarded.

   Entering a value of “0” displays Broadcast Storm Control on the port.

6. Type **S** to select Save Configuration Changes.

   Your changes are immediately activated on the switch.

Chapter 17
TACACS+ and RADIUS Protocols

This chapter contains the procedure for configuring the two authentication protocols TACACS+ and RADIUS. Sections in the chapter include:

- **TACACS+ and RADIUS Overview** on page 192
- **Configuring an Authentication Method** on page 195

TACACS+ and RADIUS Overview

The AT-S39 software has two standard management login accounts: Manager and Operator. The Manager account lets you change a switch's parameter settings while the Operator account only lets you view the settings. Each account has its own password. The Manager account has a default password of "friend" and the Operator account has a default password "operator."

For those networks that are managed by just one or two network managers, the standard accounts may be all you need. However, for larger networks managed by several network managers, you might want to give each manager his or her own management login account rather than have them share an account.

This is where TACACS+ and RADIUS can be useful. (TACACS+ is an acronym for Terminal Access Controller Access Control System. RADIUS is an acronym for Remote Authentication Dial In User Services.) These are authentication protocols. They can be used to transfer the task of validating management access from an AT-8000 Series switch to an authentication protocol server.

With the protocols, you can create a series of username and password combinations that define who can manage an AT-8000 Series switch.

There are three basic functions an authentication protocol provides:

- ❑ Authentication
- ❑ Authorization
- ❑ Accounting

When a network manager logs in to a switch, the switch passes the username and password entered by the manager to the authentication protocol server. The server checks to see if the username and password are valid for that switch. This is referred to as authentication.

If the combination is valid, the authentication protocol server notifies the switch and the switch completes the login process, allowing the manager to manage the switch.

If the username and password combination is invalid, the authentication protocol server notifies the switch and the switch cancels the login.

Authorization defines what a manager can do once logged in to a switch. You assign an authorization level to each username and password combination that you create on the server software. The access level will be either Manager or Operator.

The final function of the TACACS+ protocol is accounting, which is used to keep track of user activity on network devices. The AT-8000 Series switch does not support this function.

Note
The AT-S39 management software does not support the two earlier versions of the TACACS+ protocol, TACACS and XTACACS.

So what does it take to use the TACACS+ and RADIUS protocols on an AT-8000 Series switch? Here are the main points.

- First, you need to install TACACS+ or RADIUS server software on one or more of your network servers or management stations. Authentication protocol server software is not available from Allied Telesyn.
- The authentication protocol server can be on the same subnet or a different subnet as the AT-8000 Series switch. If the server and switch are on different subnets, be sure to specify a default gateway in the Administration Menu so that the switch and server can communicate with each other.
- You need to configure the TACACS+ or RADIUS server software. This involves the following:
  - Specifying the username and password combinations.
  - Assigning each combination an authorization level. This will differ depending on the server software you are using. TACACS+ controls this through the sixteen (0 to 15) different levels of the Privilege attribute. A privilege level of "0" gives the combination Operator status. Any value from 1 to 15 gives the combinationManager status.

    For RADIUS, management level is controlled by the Service Type attribute. This attribute has 11 different values, of which only two are functional with an AT-8000 Series switch. A value of Administrative for this attribute gives the username and password combination Manager access. A value of NAS Prompt assigns the combination Operator status.

Note
This manual does not explain how to configure TACACS+ or RADIUS server software. For that you need to refer to the documentation that came with the software.

By default, authentication protocol is disabled on an AT-8000 Series switch. Once you activate it, you will need to provide the following information:

- ❑ Which authentication protocol you want to use. Only one authentication protocol can be active on a switch at a time.
- ❑ IP addresses of up to three authentication servers.
- ❑ The encryption key used by the authentication servers.

Note
For more information on TACACS+, refer to the RFC 1492 standard. For more information on RADIUS, refer to the RFC 2865 standard.

Configuring an Authentication Method

To enable or disable the server-based authentication feature on the switch and to configure the TACACS+ and RADIUS settings, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.
2. From the Administration Menu, type **A** to select Server-based Authentication.

   The Authentication Menu in Figure 50 is displayed.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
              Authentication Menu

1 - Server-based Authentication ..... Disabled
2 - Authentication Method ........... TACACS+
3 - TACACS+ Configuration
4 - RADIUS Configuration

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 50 Authentication Menu

3. To enable or disable the authentication feature on the switch, type **1** to select Server-based Authentication. The following prompt is displayed:

   ```
   Server Based User Authentication (E-Enabled, D-
   Disabled) ->
   ```

4. Type **E** to enable the TACACS+ and RADIUS protocols on the switch or **D** to disable them. The default is disabled.

   If you enable the authentication feature, continue to the next step. If you disabled it, type **S** to save your change. You can now return to the Main Menu.

5. To select an authentication protocol, type **2** to select Authentication Method. The following prompt is displayed:

   ```
   Enter T-TACACS+, R-RADIUS ->
   ```

6. Type **T** to select TACACS+ or **R** for RADIUS. The default is TACACS+. Only one protocol can be active on the switch at a time.

Once you have activated the authentication feature on the switch and designated which authentication protocol you intend to use, you are ready to configure the selected protocol. If you selected TACACS+, go to Step 7. If you selected RADIUS, go to Step 8.

7. To configure TACACS+, do the following:

   a. Type **3** to select TACACS+ Configuration.

      The following menu is displayed:

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
               Authentication Menu

1 - TAC Server 1 .................. 0.0.0.0
2 - TAC Server 2 .................. 0.0.0.0
3 - TAC Server 3 .................. 0.0.0.0
4 - TAC Server Order ............... 1 2 3
5 - TAC Global Secret ..............
6 - TAC Timeout ................... 30 seconds

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 51 Authentication Menu (TACACS+)

   b. Configure the settings as needed. The settings are described below:

      1 - TAC Server 1
      2 - TAC Server 2
      3 - TAC Server 3
      Use these parameters to specify the IP addresses of up to three network servers containing TACACS+ server software. After you have entered an IP address, you will see the following prompt:

      ```
      Use per-server secret [Y/N] ->
      ```

      If you will be specifying more than one TACACS+ server and if all of the servers use the same encryption secret, you can answer No to this prompt and enter the encryption secret using the TAC Global Secret parameter.

      However, if you are specifying only one TACACS+ server or if the servers have difference encryption secrets, then respond with Yes to this prompt. You will see:

```
Enter per-server secret [max 40 characters] ->
```

Use this prompt to enter the encryption secret for the TACACS+ server whose IP address you are specifying.

4 - TAC Server Order
You use this selection to indicate the order in which you want the switch to query the TACACS+ servers for logon authentication. Of course, you can skip this option if you specified only one IP address. The default is 1, 2, and 3, in that order.

5 - TAC Global Secret
If all of the TACACS+ servers have the same encryption secret, rather then entering the same secret when you enter the IP addresses, you can use this option to enter the secret just once.

3 - TAC Timeout
This parameter specifies the maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there aren't any more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

c. After you have finished configuring the parameters, type **S** to select Save Configuration Changes.

8. To configure the RADIUS protocol, from the Authentication Menu in Figure 50 on page 195 do the following:

   a. Type **4** to select RADIUS Configuration.

The following menu is displayed:

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
           RADIUS Client Configuration

1 - Global Encryption Key ............. 0.0.0.0
2 - Global Server Timeout period....... 0.0.0.0
3 - RADIUS Server 1 Configuration ..... 0.0.0.0
4 - RADIUS Server 2 Configuration ..... 0.0.0.0
5 - RADIUS Server 3 Configuration ..... 0.0.0.0
6 - Show Status

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 52 RADIUS Client Configuration

b. Configure the parameters as needed. The parameters are defined below:

Global Encryption Key
This parameter specifies the encryption key for the RADIUS servers. This option is useful if you will be entering more than one RADIUS server and all the servers share the same encryption key. If the servers use different encryption keys, leave this option blank.

Global Server Timeout period
This parameter specifies the maximum amount of time the switch will wait for a response from a RADIUS server before assuming that the server cannot respond. If the timeout expires and the server hasn't responded, the switch queries the next RADIUS server in the list. If there aren't any more servers, than the switch will default to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

3 - RADIUS Server 1 Configuration
4 - RADIUS Server 1 Configuration
5 - RADIUS Server 1 Configuration
Use these parameters to specify the IP addresses of up to three network servers containing the RADIUS server software. Selecting one of the options displays the following menu:

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
          RADIUS Server 1 Configuration

1 - Server IP Address ................. 0.0.0.0
2 - Server Authentication UDP Port .... 1812
3 - Server Encryption Key ........ <Not Defined>

S - Save Configuration Changes
R - Return to Previous Menu

Enter your selection?
```

Figure 53 RADIUS Server Configuration

The options are described below:

1 - Server IP Address
Use this option to specify the IP address of the RADIUS server.

2 - Server Authentication UDP Port
Use this option to specify the UDP port of the RADIUS protocol.

3 - Server Encryption Key
Use this option to specify the encryption key for the RADIUS server.

c. After you have finished configuring the parameters, type **S** to select Save Configuration Changes.

Chapter 18
802.1x Port-Based Network Access Control

This chapter contains an overview and procedures for 802.1x Port-based Network Access Control features. Sections are as follows:

- ❑ **Port Access Control Overview** on page 201
- ❑ **Enabling and Disabling Port Access Control** on page 203
- ❑ **Type S to select Save Configuration Changes.** on page 203
- ❑ **Configuring Port Access Control Parameters** on page 204
- ❑ **Viewing Port Access Status** on page 207

Port Access Control Overview

The AT-S39 software's IEEE 802.1X-based Port Access Control feature is a client-server-based access control and authentication protocol that restricts unauthorized clients who attempt to connect to a network through accessible, local ports. When Port Access Control is enabled, the authentication server authenticates each client connected to a port before making available the network or any services offered by the switch.

The following sections describe the following device roles in EEE 802.1X port-based authentication:

- Client
- Switch
- Authentication Server

Client

The client is the device that requests access to the network and switch and responds to requests from the switch.In the IEEE 802.1X specification, the client is referred to a s the supplicant.

Switch

When Port Access Control is enabled, the switch controls access to the network based on the authentication status of the client. The switch acts as an intermediary between the client and the authentication server, identity information is requested from the client, the information is verified with the authentication server, and a response is relayed to the client. In the IEEE 802.1X specification, the switch is referred to a s the authenticator.

Authentication Server

The authentication server authenticates the identity of the client. After the identity of the client has been validated, the authentication server notifies the switch whether or not the client is authorized to access the network.

Because the switch is the intermediary, the authentication server is transparent to the client. Remote Authentication Dial-In User Service (RADIUS) with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server. For more information on RADIUS, refer to **TACACS+ and RADIUS Protocols** on page 191.

When the switch receives frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is reencapsulated in the RADIUS format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

For information on RADIUS, refer **TACACS+ and RADIUS Protocols** on page 191,

Note
Port access control can only be configured via local and Telnet management.

The following sections describe procedures for configuring Port Access Control.

Enabling and Disabling Port Access Control

To globally enable or disable Port Access Control, perform the following procedure:

Note
Enabling or disabling Port Access Control can only be performed in a local management session.

Note
Before activating this feature, you must have the RADIUS EAP specified and enabled as the authenication method. This is discussed in **Configuring an Authentication Method** on page 195.

1. From the Main Menu, type **1** to select Port Menu (shown in Figure 54).
2. Type **6** to select Port Access Control (shown in Figure 54).

```
      Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
                  Port Access Control

1 - Port Access Control ..............  Enabled
2 - Authentication Method ............  RADIUS EAP
3 - Configure Port Access Parameters
4 - Display Port Access Parameters
5 - Display Port Access Status

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 54 Port Access Control Menu

3. Type **1** to select Port Access Control. The following prompt is displayed:

   ```
   Port Access Control (E-Enable, D-Disable) :
   ```

4. Type **E** to enable port access control, or **D** to disable port access control. Press Return.
5. Type **S** to select Save Configuration Changes.

Configuring Port Access Control Parameters

To configure port access control parameters, perform the following procedure:

1. From the main menu, type **1** to select the Port menu.
2. In the Port menu, type **6** to select the Port Access Control menu.
3. In the Port Access Control Menu, type **3** to select Configure Port Access Parameters. The following prompt is displayed:

   ```
   Enter ports list ->
   ```

4. Enter the port or the range of ports that you want to configure. Press Return. The following menu is displayed.

```
      Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
            Configure Port Access Parameters

Configuring Ports 3
0 - Port Role ......... None

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 55 Configuring Port Access

5. Type **0** to select Port Role. The following prompt is displayed:

   ```
   Enter new port role [N-None,A-Authenticator] ->
   ```

6. Type **A** to select Authenticator. Press Return. Additional Configure Port Access Parameters are displayed (see Figure 56). Port Access Parameters are listed as menu items with factory set default ranges.

```
      Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
            Configure Port Access Parameters

Configuring Ports 3
0 - Port Role ......... Authenticator
1 - Port Control ...... Auto
2 - quietPeriod ....... 60
3 - txPeriod .......... 30
4 - reAuthPeriod ...... 3600
5 - suppTimeout ....... 30
6 - serverTimeout ..... 30
7 - maxReq ............ 2

S - Save Configuration changes
R - Return to Previous Menu

Enter your selection?
```

Figure 56 Configure Port Access Parameters Menu

7. Select the parameter that you wish to modify. The parameters are described below:

   0 - Port Role
   This parameter specifies the current authentication status of the port . If Authenticator is selected, the port performs the role of authenticating the supplicants that are connected to the port. If None is selected, the port does not participate in port access control. The default for this parameter is None.

   1 - Port Control
   This parameter can take the following values:

   - **Force-authorized**: Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This is the default setting
   - **Force-unauthorized**: Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface

- **Auto**: Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes . The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client that attempts to access the network is uniquely identified by the switch by using the client's MAC address.

2 - quietPeriod
Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

3 - txPeriod
Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

4 - reAuthPeriod
Enables periodic reauthentication of the client, which is disabled by default. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

5 - suppTimeout
Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

6 - serverTimeout
This is the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 30 seconds. The range is 1 to 65,535 seconds.

7 - maxReq
This parameter specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

8. Type **S** to select Save Configuration Changes.

Viewing Port Access Status

To view port access status, perform the following procedure:

1. From the main menu, type **1** to select the Port menu.
2. In the Port menu, type **6** to select the Port Access Control menu.
3. From the Port Access Control Menu, type **5** to select Display Port Access Status. The Port Access Status is displayed (see Figure 57).

```
      Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
               Display Port Access Status

Port   PortRole        Status           Supplicant
-------------------------------------------------------
001  None            ------          -----------------
002  Authenticator   ------          -----------------
003  Authenticator   ------          -----------------
004  Authenticator   ------          -----------------
005  None            ------          -----------------
006  None            ------          -----------------
007  None            ------          -----------------
008  None            ------          -----------------

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 57 Display Port Access Status Menu

Chapter 19
Ethernet Statistics

This chapter contains the procedures for displaying data traffic statistics. Sections in the chapter include:

- **Displaying Port Statistics** on page 209
- **Displaying Switch Statistics** on page 211

Displaying Port Statistics

To display Ethernet port statistics, perform the following procedure:

1. From the Main Menu, type **7** to select Ethernet Statistics.

   The Ethernet Statistics menu in Figure 58 is displayed.

```
     Allied Telesyn AT-8024 Ethernet Switch
Login Sesion: Manager
              Ethernet Statistics


1 - Display Port Statistics
2 - Display Module Statistics
3 - Clear Statistics

R - Return to Previous Menu

Enter your selection?
```

Figure 58 Ethernet Statistics Menu

2. From the Ethernet Statistics menu, type **1** to select Display Port Statistics.

   A window is displayed containing the statistics for each port. The information in this window is for viewing purposes only. The statistics are defined below:

   Total Count
   Number of bytes received and transmitted on the port.

   Transmit Packets (TX_COUNT)
   Number of bytes transmitted out the port.

   Received Packets (RX_COUNT)
   Number of bytes received on the port.

   Received Broadcast (RX_BRDCAST)
   Number of broadcast packets received on the port.

   Received Multicast (RX_MLTCAST)
   Number of multicast packets received on the port.

   Received Unicast (RX_UNICAST)
   Number of unicast packets received on the port.

   Received Overflow (RX_OVERFLOW)
   Number of times the capacity of the port's buffer has been exceeded.

CRC Error (CRC_ERROR)
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Undersize Packets (UNDERSIZE)
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Packets (OVERSIZE)
Number of packets exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Fragmented Packets (FRAGMENT)
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Port in Discards (PRT_DISCARD)
Number of frames successfully received and buffered by the port, but discarded and not forwarded.

If you want to clear the counters on the port and return them to “0”, select the option “3 - Clear Statistics” from the Ethernet Statistics menu.

Displaying Switch Statistics

To display Ethernet statistics for an entire switch, perform the following procedure:

1. From the Main Menu, type **7** to select Ethernet Statistics.
2. From the Ethernet Statistics menu, type **2** to select Display Module Statistics.

   The statistics for the port are displayed in the Display Module Statistics window, shown in Figure 59.

```
     Allied Telesyn Ethernet Switch AT-8024
Login Privilege: Manager
           Display Module Statistics


Ethernet statistics for this module
TOTAL_COUNT ................. 0
TX_COUNT .................... 0
RX_COUNT .................... 0
RX_BRDCAST .................. 0
RX_MLTCAST .................. 0
RX_UNICAST .................. 0
RX_OVERFLOW ................. 0
CRC_ERROR ................... 0
UNDERSIZE ................... 0
OVERSIZE .................... 0
FRAGMENT .................... 0
PORT_IN_DISCARDS ............ 0


U - Update Display
C - Clear Module Statistics
R - Return to Previous Menu


Enter your selection?
```

Figure 59 Display Module Statistics Window

The information in this window is for viewing purposes only. The statistics are defined below:

Total Count
Number of valid packets received and transmitted by the switch.

Transmit Packets
Number of packets transmitted from the switch.

Received Packets
Number of packets received by the switch.

Received Overflow
Number of times the capacity of the port buffers have been exceeded.

Received Broadcast
Number of broadcast packets received on the switch.

Received Multicast
Number of multicast packets received on the switch.

CRC Error
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received by the switch.

Undersize Packets
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the switch.

Fragmented Packets
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the switch.

Oversize Packets
Number of packets exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the switch.

Port in Discards
Number of frames successful received and buffered by the switch, but discarded and not forwarded.

If you want to clear the counters on the switch and return them to “0”, select the option “3 - Clear Statistics” from the Ethernet Statistics Menu.

Chapter 20
File Downloads and Uploads

There are three files that coexist on an AT-8000 Series switch while the device is operating. They are:

- AT-S39 management software

  This is the operating software for the switch.

- AT-S39 bootloader

  This image contains the code that initially controls the switch whenever you power on or reset the unit.

- Switch configuration file

  This file contains the settings for the different switch parameters. such as VLANs, STP settings, and so forth.

Note
In versions previous to AT-S39 Version 2.0.1, the management software and bootloader were offered as separate files. In all later versions, the files are combined into one image file.

You can use the AT-S39 management software to download new versions of the management software and bootloader onto a switch so that a switch always has the latest software.

You can also upload a configuration file from a switch onto a management workstation and then download it onto another switch. This can be useful in network environments containing a large number of AT-8000 Series switches that will all be configure the same, or nearly

the same. What you can do is configure one of the AT-8000 Series switches in your network, and then download its configuration file to the other switches. This can save you the trouble of having to configure each switch individually.

There are a several different ways for downloading and uploading files onto a switch. They are:

- Local management session

  One method for downloading or uploading files is from a local management session on the switch using either Xmodem or TFTP. The procedure for this is explained in **Transferring Files from a Local Management Session** on page 216.

- Remote management session

  Another method for downloading or uploading files is from a remote Telnet management session on the switch using TFTP. The procedure for this is explained in **Transferring Files from a Telnet Session** on page 220.

- Switch to switch

  This procedure is useful if you have a large number of AT-8000 Series switches in your network. What you can do is upgrade the software on one master switch and then instruct the master switch to upgrade the software in the other switches in the same subnet. This procedure is explained in **Downloading Files Switch to Switch** on page 223.

Obtaining Software Updates

New releases of the AT-S39 management software are available from the Allied Telesyn web site at www.alliedtelesyn.com and our FTP server at ftp.alliedtelesyn.com. To log on to the FTP server, enter "anonymous" for the user name and your email address for the password. Management software for these switches will have "S39" as part of the filename.

Note
All switch models in the AT-8000 Series use the same management software image.

Transferring Files from a Local Management Session

This section contains the procedure for downloading or uploading the following files onto a switch from a local management session.

- ❑ New AT-S39 software image and bootloader software
- ❑ Configuration file

You can transfer a file using Xmodem or TFTP. In order to use TFTP, there must be a node on your network with the TFTP server software and the file to download must be stored on the same node.

Caution
The switch will stop forwarding Ethernet traffic during the download of the AT-S39 software image.

Note
Installing a new AT-S39 software image does not change the current configuration of a switch (e.g., IP address, subnet mask, and virtual LANs). To return a switch to its default configuration values, refer to **Returning the AT-S39 Software to the Factory Default Values** on page 54.

This procedure assumes that you have already obtained the new software from Allied Telesyn and stored it on the management workstation from which you will be performing the procedure, or on the TFTP server.

To download a new software image or configuration file onto a switch, perform the following procedure:

1. Establish a local management session on the switch where you intend to download the new management software or configuration file.

   For instructions, refer to **Starting a Local Management Session** on page 30.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The following menu is displayed:

```
      Allied Telesyn Ethernet Switch AT-8024
Login Session: Manger
               Downloads & Uploads


1 - Download Application Image/Bootloader
2 - Download Configuration Data

3 - Upload Application Image
4 - Upload Configuration Data

R - Return to Previous Menu

Enter your selection?
```

Figure 60 Downloads & Uploads Menu

Note
Options 3 and 4 in the menu are described in **Uploading Files** on page 225.

4. To download a new software image and bootloader onto the switch, type **1**. To download a configuration file, type **2**.

   The following prompt is displayed:

   ```
   Download Method/Protocol [X-Xmodem, T-TFTP]:
   ```

5. To download a file using Xmodem, go to Step 6. To download a file using TFTP, do the following:

   a. Type **T**.

      The following prompt is displayed:

      ```
      TFTP Server IP address:
      ```

   b. Enter the IP address of the TFTP server.

      The following prompt is displayed:

      ```
      Remote File Name:
      ```

   c. Enter the directory path and file name of the image file or configuration file that you want to download.

Note
If you are installing a new management image, the switch begins to initialize the software after it is installed, a process that takes approximately one minute to complete. Once the management software is initialized, the switch automatically resets.

6. To download a file using Xmodem, type **X** at the prompt displayed in Step 4.

   The following prompt is displayed:

   ```
   You are going to invoke the Xmodem download utility.
   Do you wish to continue? [Yes/No]

   Note:Please select 1K Xmodem protocol for faster
   download.
   ```

7. Type **Y** for Yes.

   The prompt “Downloading” is displayed.

8. Begin the file transfer of the new management software image.

   Note
   The transfer protocol must be Xmodem or 1K Xmodem.

   Steps 9 through 12 illustrate how you would download a file using the Hilgraeve HyperTerminal program.

9. From the HyperTerminal main window, select the **Transfer** menu. Then select **Send File** from the pull-down menu, as shown in Figure 61.

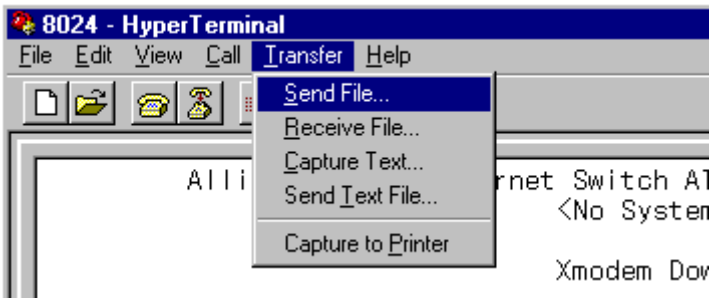

Figure 61 Local Management Window

The Send File window in Figure 62 is displayed.

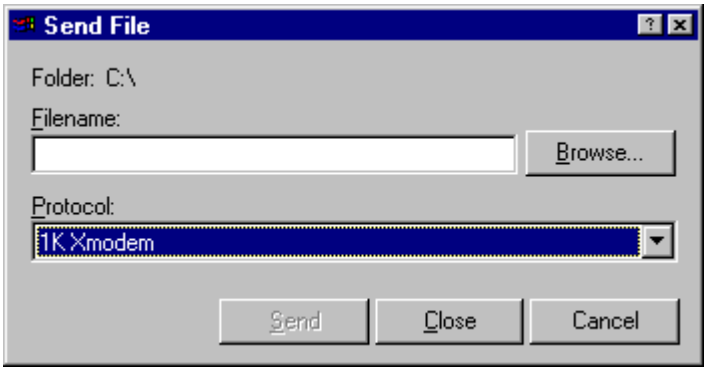

Figure 62 Send File Window

10. Click the Browse button and specify the location and file to be downloaded onto the switch.
11. Click on the Protocol field and select as the transfer protocol either Xmodem or, for a faster download, 1K XModem.
12. Click Send.

    The software immediately begins to download onto the switch. The Xmodem File Send window in Figure 63 displays current status of the software download. The download process takes a couple minutes to complete.

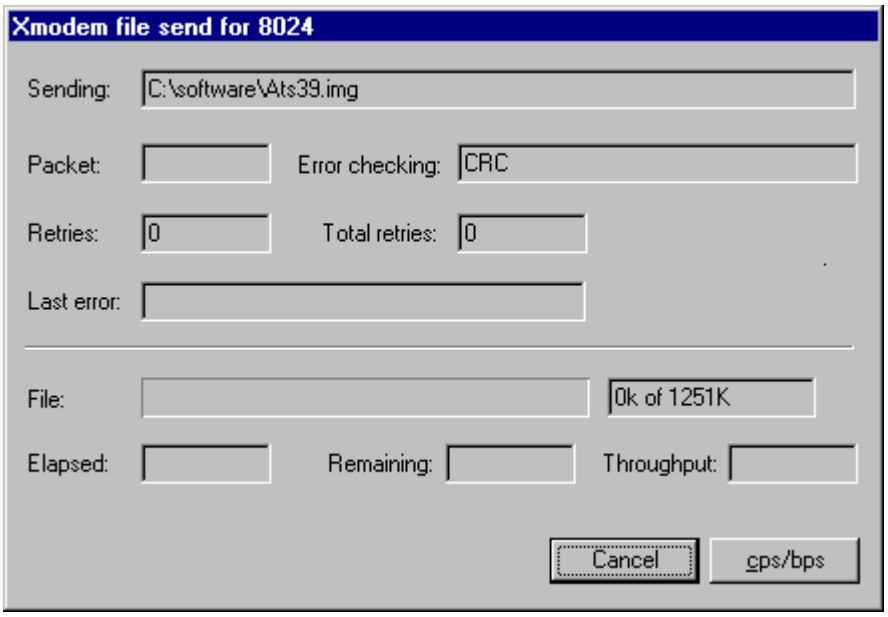

Figure 63 XModem File Send Window

If you are installing a new management image, the switch begins to initialize the software after it is installed, a process that takes approximately one minute to complete. Once the management software is initialized, the switch automatically resets.

Note
Do not interrupt the initialization process. Do not reboot the switch.

Transferring Files from a Telnet Session

This section contains the procedure for downloading or uploading the following files onto a switch from a Telnet session.

- ❑ New AT-S39 software image and bootloader software
- ❑ Configuration file

You can transfer a file using TFTP. To use TFTP, there must be a node on your network with the TFTP server software and the file to download must be stored on the same node.

⚠ Caution
The switch will stop forwarding Ethernet traffic during the download of the AT-S39 software image.

Note
Installing a new AT-S39 software image does not change the current configuration of a switch (e.g., IP address, subnet mask, and virtual LANs). To return a switch to its default configuration values, refer to **Returning the AT-S39 Software to the Factory Default Values** on page 54.

This procedure assumes that you have already obtained the new software from Allied Telesyn and stored it on the TFTP server.

To download a new software image or configuration file onto a switch, perform the following procedure:

1. Establish a Telnet management session on the switch where you intend to download the new management software or configuration file.

   For instructions, refer to **Starting a Telnet Management Session** on page 34.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The following menu is displayed:

```
     Allied Telesyn Ethernet Switch AT-8024
Login Session: Manger
               Downloads & Uploads


1 - Download Application Image/Bootloader
2 - Download Configuration Data

3 - Upload Application Image
4 - Upload Configuration Data

R - Return to Previous Menu

Enter your selection?
```

Figure 64 Downloads & Uploads Menu

Note
Options 3 and 4 in the menu are described in **Uploading Files** on page 225.

4. To download a new software image and bootloader onto the switch, type **1**. To download a configuration file, type **2**.

   The following prompt is displayed:

   ```
   Download Method/Protocol [T-TFTP] :
   ```

   a. Type **T**.

      The following prompt is displayed:

      ```
      TFTP Server IP address:
      ```

   b. Enter the IP address of the TFTP server.

      The following prompt is displayed:

      ```
      Remote File Name:
      ```

   c. Enter the directory path and file name of the image file or configuration file that you want to download.

Note
The image file and configuration file must be stored on the TFTP server. Additionally, the paths to these files must be specified in the TFTP server.

Once the filename has been specified, the download begins. File download takes only a few moments.

Note
If you are installing a new management image, the switch begins to initialize the software after it is installed, a process that takes approximately one minute to complete. Once the management software is initialized, the switch automatically resets, disconnecting the current telnet management session. After allowing the switch to reset, the user must reestablish the Telnet management session.

Downloading Files Switch to Switch

The previous procedure explained how to download an AT-S39 software image or configuration file onto a switch from a local management session. This procedure explains how to download an AT-S39 software image or configuration file from one AT-8000 Series switch to another switch.

This procedure is useful in networks that contain a large number of AT-8000 Series switches. Once you have updated the software on the master switch of an enhanced stack, you can instruct the master switch to automatically upgrade the other AT-8000 Series switches in the same subnet.

> **Note**
> The following procedure can only be performed from a local management session.

To download a management software image or configuration file from a master switch to other switches in the same subnet, perform the following procedure:

1. From the Main Menu, type **9** to select Enhanced Stacking.

   The Enhanced Stacking window in Figure 10 on page 61 is displayed.

2. From the Enhanced Stacking window, type **2** to select Stacking Services.

   > **Note**
   > The "2 - Stacking Services" selection is available only on master switches.

   The window in Figure 11 on page 63 is displayed.

3. Do one of the following:

   - ❑ To download both the AT-S39 software image and bootloader on the master switch to another AT-8000 Series switch, type **I** to select Image Download to Remote Switches.
   - ❑ To download the configuration file on the master switch to another AT-8000 Series switch, type **C** to select Config Download to Remote Switches.
   - ❑ To download just the bootloader on the master switch to another switch, type **B** to select Bootloader Download to Remote Switches.

The following prompt is displayed:

```
Enter the starting remote switch number -> [1 to 12]
```

4. Enter the number of the switch whose software or configuration file you want to update. To update a range of switches, enter the number of the first switch.

   The following prompt is displayed:

   ```
   Enter the ending remote switch number -> [1 to 12]
   ```

5. Enter the last switch in the range you want to update. To update just one switch, enter the same number here as you entered in the previous step.

   The following prompt is displayed:

   ```
   Do you want to show remote switch burning flash ->
   [Yes/No]
   ```

6. You can respond with Yes or No to this prompt. It does not affect the download.

   The following prompt is displayed:

   ```
   Do you want confirmation before downloading each
   switch -> [Yes/No]
   ```

7. Answering Yes to this prompt means that the management software will prompt you with a confirmation message before it begins to upgrade each switch. Answering No means the management software will not display a confirmation prompt before downloading.

   The management software begins the download. The management software notifies you when the download is complete.

⚠ Caution

Once a switch image file has been downloaded, the switch must decompress it and write it to flash. This can require one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file. Once the file has been decompressed, the switch automatically resets.

Uploading Files

To upload a management software image or configuration from a switch onto your management station, perform the following procedure:

> **Note**
> It is not recommended that you upload an AT-S39 software image onto a management workstation for download onto another switch. New AT-S39 software images for downloading onto a switch should only be obtained from the Allied Telesyn web site.

1. Start a local management session on the switch where you intend to upload the management software image or configuration file.

   For instructions, refer to **Starting a Local Management Session** on page 30.

2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

   The Downloads and Uploads menu in Figure 60 on page 217 is displayed.

4. To upload the AT-S39 software image and bootloader from the switch, type **3**. To upload a configuration file, type **4**.

   The following prompt is displayed:

   ```
   Download Method/Protocol [X-Xmodem, T-TFTP]:
   ```

5. To upload a file using Xmodem, go to Step 6. Upload a file using TFTP, do the following:

   a. Type **T**.

      The following prompt is displayed:

      ```
      TFTP Server IP address:
      ```

   b. Enter the IP address of the TFTP server.

      The following prompt is displayed:

      ```
      Remote File Name:
      ```

   c. Enter the file name that the image file or configuration file is to be stored under on the TFTP server.

      Once the filename has been specified, the upload begins. Uploading a configuration file takes only a few moments. Uploading an AT-S39 image file can take several minutes.

Section III
Web Browser Management

The chapters in this section explain how to manage an AT-8024 or AT-8024GB Fast Ethernet switch using a web browser. The chapters include:

- **Chapter 21, Starting a Web Browser Management Session** on page 227
- **Chapter 22, Basic Switch Parameters** on page 231
- **Chapter 23, Enhanced Stacking** on page 244
- **Chapter 24, Port Parameters** on page 249
- **Chapter 25, Port Security** on page 258
- **Chapter 26, Port Trunks** on page 260
- **Chapter 27, Port Mirroring** on page 263
- **Chapter 28, STP and RSTP** on page 266
- **Chapter 29, Virtual LANs** on page 278
- **Chapter 30, MAC Address Table** on page 289
- **Chapter 31, Class of Service** on page 296
- **Chapter 32, IGMP Snooping** on page 298
- **Chapter 33, Broadcast Storm Control** on page 304
- **Chapter 34, TACACS+ and RADIUS Protocols on page 307**

Chapter 21
Starting a Web Browser Management Session

This chapter contains the procedure for starting a management session on an AT-8000 Series switch using a web browser, such as Microsoft Internet Explorer or Netscape Navigator.

Starting a Web Browser Management Session

This section explains how to start a web browser management session.

There must be at least one AT-8000 Series switch on your network that has been assigned an IP address. The switch with the IP address is referred to as the master switch. Once you have started a Telnet management session on the master switch, you will have management access to all other AT-8000 Series switches that reside in the same subnet.

> **Note**
> For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

> **Note**
> If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser's network options not to use proxies. Consult your web browser's documentation on how to configure the switch's web browser not to use proxies.

2. Enter the IP address of the master switch of the enhanced stack in the URL field of the browser, as shown in Figure 65.

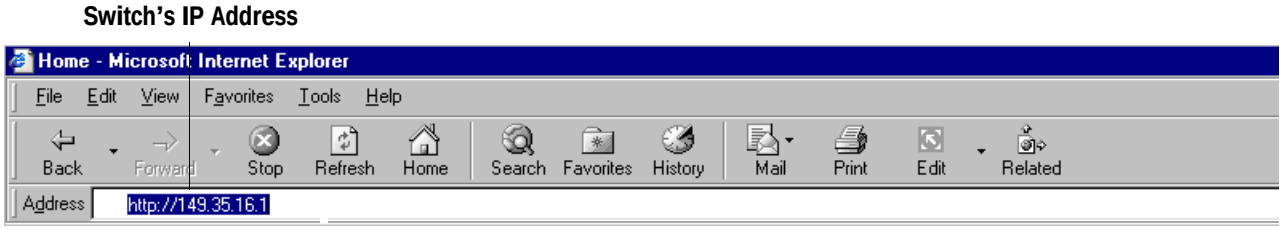
Switch's IP Address
Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Related
Address http://149.35.16.1

Figure 65 Entering a Switch's IP Address in the URL Field

3. When prompted, enter a user name and password. For manager access, enter "manager" as the user name. The default password is "friend". For operator access, enter "operator" as the user name. The default password is "operator". Logins and passwords are case-sensitive. (For information on the two access levels, refer to **Management Access Levels** on page 25.)

The user names cannot be changed. To change a password, refer to **Configuring an IP Address and Switch Name** on page 39.

The window shown in Figure 66 is displayed.

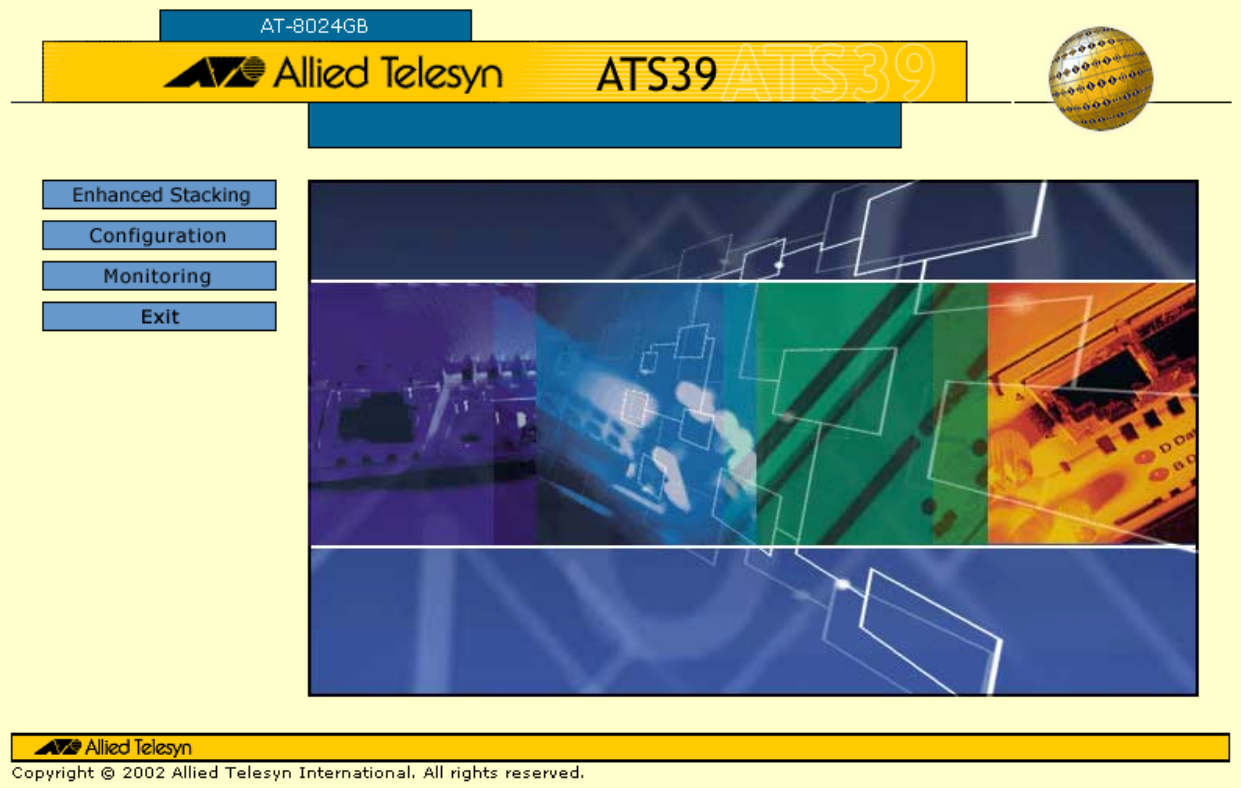

Figure 66 Home Page

This is the Home page of the management software. In the left portion of the Home page is the main menu:

- Configuration
- Monitoring
- Exit

Note
A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit the browser.

Browser Tools

You can use the browser tools to move around the Omega menus. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature on frequently-used Omega menus and windows.

Quitting from a Web Browser Management Session

To exit from a web browser management session, return to the Home page and select Exit from the main menu.

Chapter 22
Basic Switch Parameters

This chapter contains the following sections:

- **Configuring an IP Address and Switch Name** on page 232
- **Activating the BOOTP and DHCP Services** on page 236
- **Viewing System Information** on page 237
- **Configuring the SNMP Parameters and Trap IP Addresses** on page 239
- **Resetting a Switch** on page 241
- **Pinging a Remote System** on page 242
- **Returning the AT-S39 Software to the Factory Default Values** on page 243

Configuring an IP Address and Switch Name

Note
For guidelines on when to assign an IP address, subnet address, and gateway address to an AT-8024 or AT-8024GB switch, refer to **When Does a Switch Need an IP Address?** on page 37.

To set the basic switch parameters for an AT-8024 or AT-8024GB Fast Ethernet switch, perform the following procedure:

1. From the Home Page, select **Configuration**.

   The Configuration menu is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the **General** tab.

The General tab in Figure 67 is displayed.

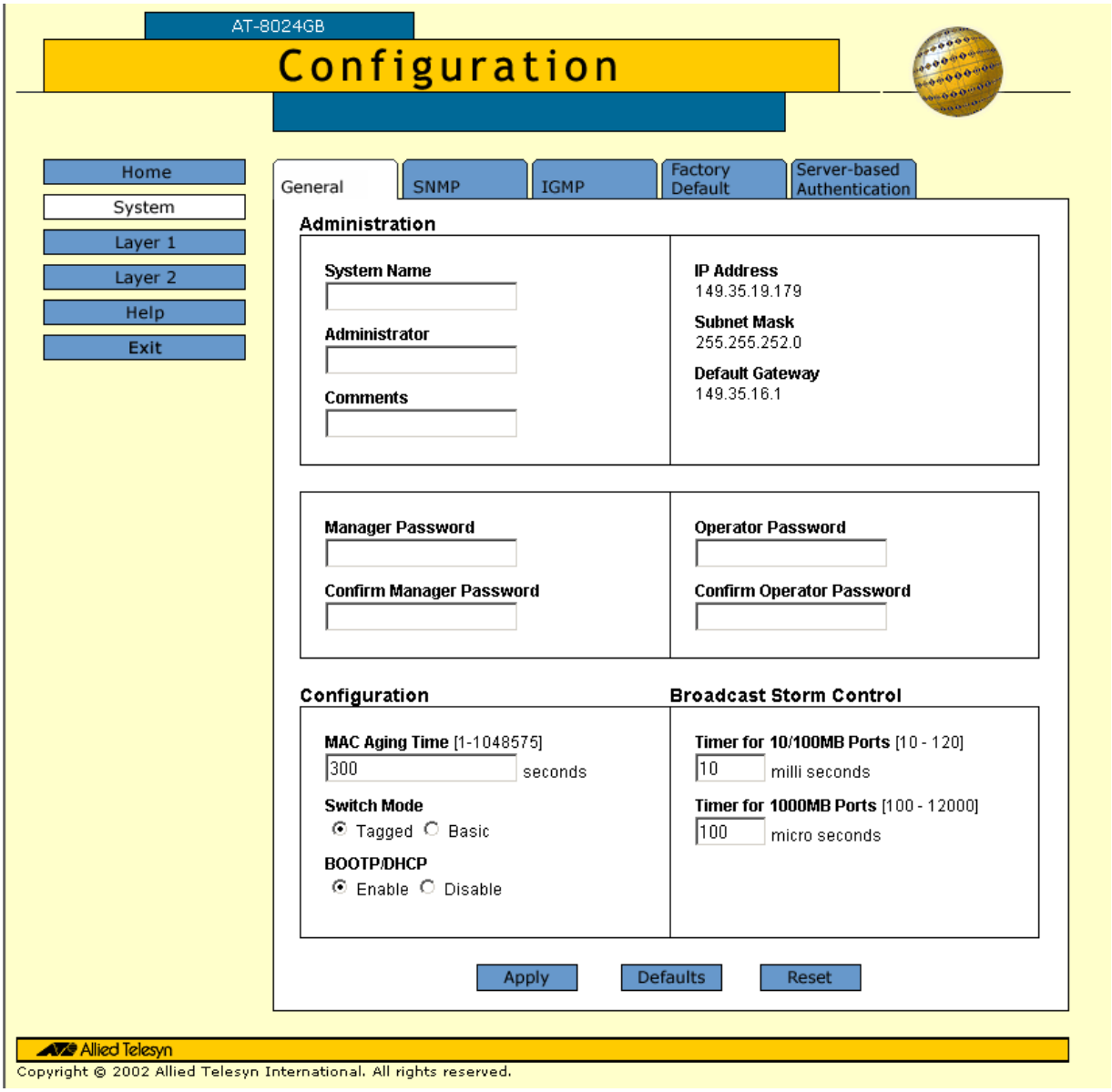

Figure 67 General Tab Menu - Configuration

Note
This procedure describes the parameters in the Administration section of the menu. The parameters in the Configuration and Broadcast Storm Control sections are discussed later in this guide.

Note
The Reset button at the bottom of the menu is used to reset the switch.

3. Change the parameters as desired.

   The parameters are described below:

   System Name
   This parameter specifies a name for the switch (for example, Sales Ethernet switch). Entering a value for this parameter is optional.

   Note
   You should assign each switch a name. The names can help you identify the various switches in your network. This can help you avoid performing a configuration procedure on the wrong switch.

   Administrator
   This parameter specifies the name of the network administrator responsible for managing the switch. Entering a value for this parameter is optional.

   Comments
   This parameter specifies additional information about the Fast Ethernet switch, such as its location (e.g., Floor 4, Wiring closet 402B). Entering a value for this parameter is optional.

   Manager Password
   Manager Confirm Password
   These parameters are used to change the administrator's login password for the switch. The password can be from 0 to 20 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password is "admin".

   Caution
   You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

   Operator Password
   Operator Confirm Password
   These parameters are used to change the operator's login password for the switch. The password can be from 0 to 20 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password for operator is "operator".

Caution
You should not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

IP address
This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program.

Subnet mask
This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch.

Gateway address
This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router.

4. After you have set the parameters, click Apply. Your changes are not stored by the switch until you select Apply.

Note
A change to any of the above parameters, including the IP address and subnet mask, is immediately activated on the switch.

A change to the IP address of the switch will result in the loss of the remote management session. You can restart the management session using the switch's new IP address.

Activating the BOOTP and DHCP Services

For background information on BOOTP and DHCP, refer to the section **Activating the BOOTP and DHCP Services** on page 42.

To activate or deactivate the BOOTP and DHCP protocols on the switch from a web browser management session, perform the following procedure:

1. From the Home Page, select **Configuration**.

   The Configuration menu is displayed with the System menu option selected by default.

2. If the System menu option is not selected, select it and then select the **General** tab.

   The General Tab menu is displayed, as shown in Figure 67 on page 233.

3. In the BOOTP/DHCP options in the General tab menu, click either **Enable** or **Disable**.

   Note
   If you activated BOOTP/DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response.

Viewing System Information

To view basic information about the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **System**.
3. Select the **General** tab.

   The General tab window in Figure 68 is displayed.

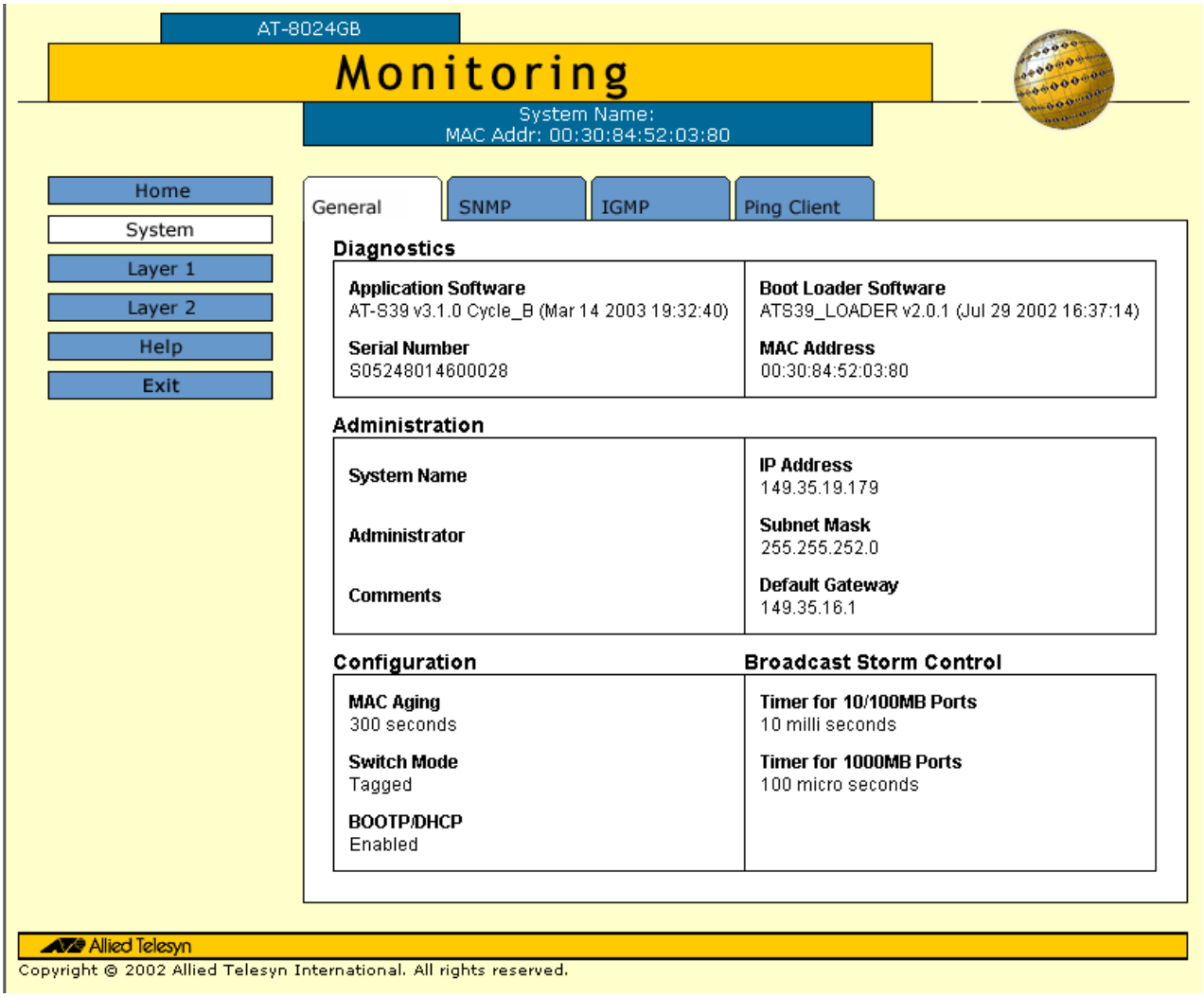

Figure 68 General Tab Window - Monitoring

This window is for viewing purposes only. You cannot change any of the values from this window. The sections in the window are defined below.

General
This section displays the switch's serial number and the switch's MAC address. These values cannot be changed.

Administration
This section contains a variety of information, including the IP address of the switch and the system name. These parameters are defined in the procedure **Configuring an IP Address and Switch Name** on page 232, which also explains how to change the parameters.

Configuration
This section contains the following items:

- MAC Aging - Specifies how long an inactive dynamic MAC address can remain in the MAC address table before it is deleted. The default is 300 seconds (5 minutes). For background information about MAC addresses, refer to **MAC Address Overview** on page 162.

- Switch Mode - Defines the switch's current VLAN mode. If this parameter displays "Tagged," the switch supports port-based and tagged VLANs. If this parameter displays "Basic," the switch is operating in the Basic Mode. For information about VLANs, refer to the overview sections in **Chapter 10, Virtual LANs Overview** on page 115.

- BOOTP/DHCP - Defines whether the switch obtains its IP address from a BOOTP or DHCP server on your network. If this parameter is enabled, the switch obtains its IP address from a BOOTP or DHCP server.

Configuring the SNMP Parameters and Trap IP Addresses

To change the switch's SNMP community strings or to specify the IP addresses of management stations to receive traps from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **System**.
3. Select the **SNMP** tab.

   The SNMP menu in Figure 69 is displayed.

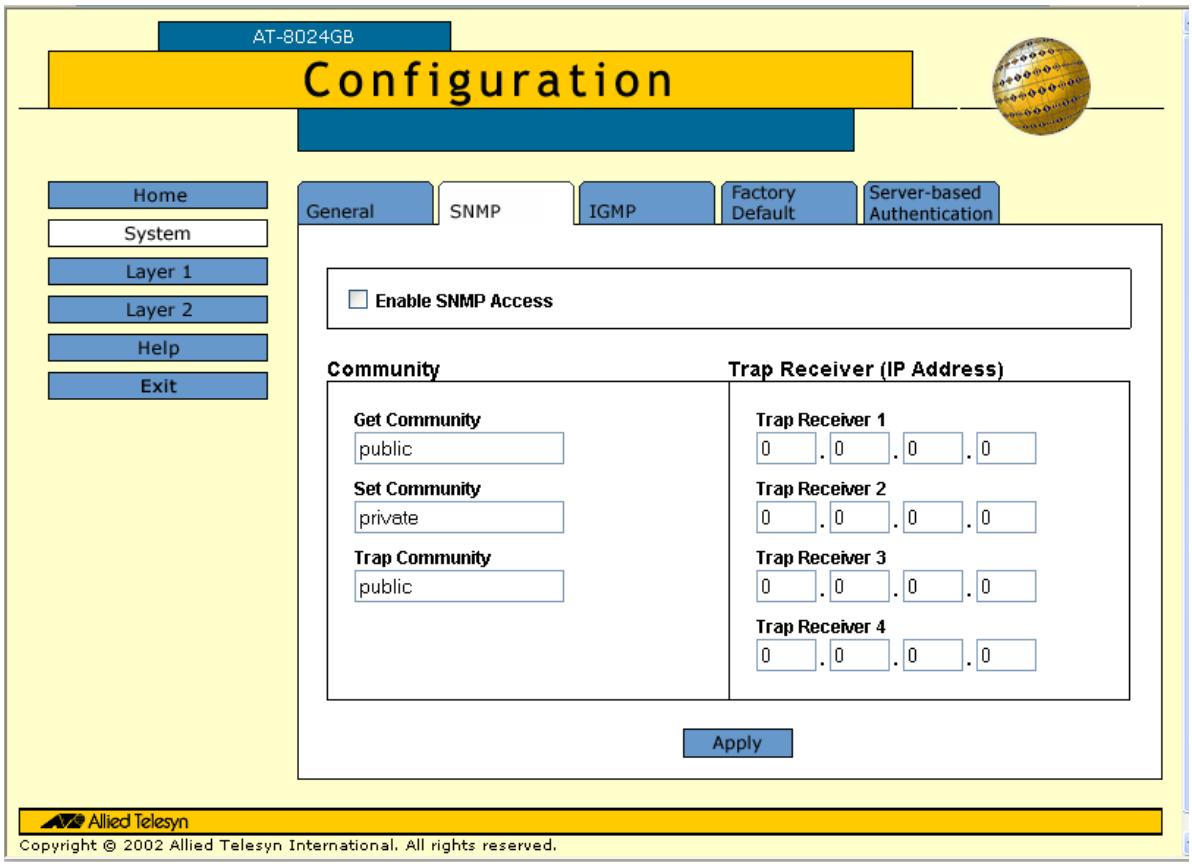

Figure 69 SNMP Tab

4. Adjust the parameters as desired. The parameters are described below.

   GET Community
   SET Community
   Trap Community
   Use these parameters to set a switch's SNMP community strings.

Trap Receiver 1
Trap Receiver 2
Trap Receiver 3
Trap Receiver 4
Use these selections to specify the IP addresses of up to four management workstations on your network to receive traps from the switch.

Note
The Enable SNMP Access check box in the menu controls whether the switch can be remotely managed using an SNMP application program. If the check box is empty, the switch cannot be managed through SNMP. This is the default.

5. Click **Apply** to save your changes to the switch.

   Changes are immediately activated on the switch.

Resetting a Switch

To reset a switch, perform the following procedure:

1. From the Home Page, select **Configuration**.

   The Configuration menu is displayed with the System option selected by default.

2. If the System menu option is not selected, select it and then select the **General** tab.

3. Click the **Reset** button at the bottom of the menu.

   A confirmation prompt is displayed.

4. Click **OK** to reset the switch or **Cancel** to cancel the procedure.

   Resetting the switch ends your web browser management session. You must restart the session to continue managing the switch.

Pinging a Remote System

You can instruct the switch to ping a node on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring menu, select the **System** menu option.
3. Select the **Ping Client** tab.

   The menu in Figure 70 is displayed.

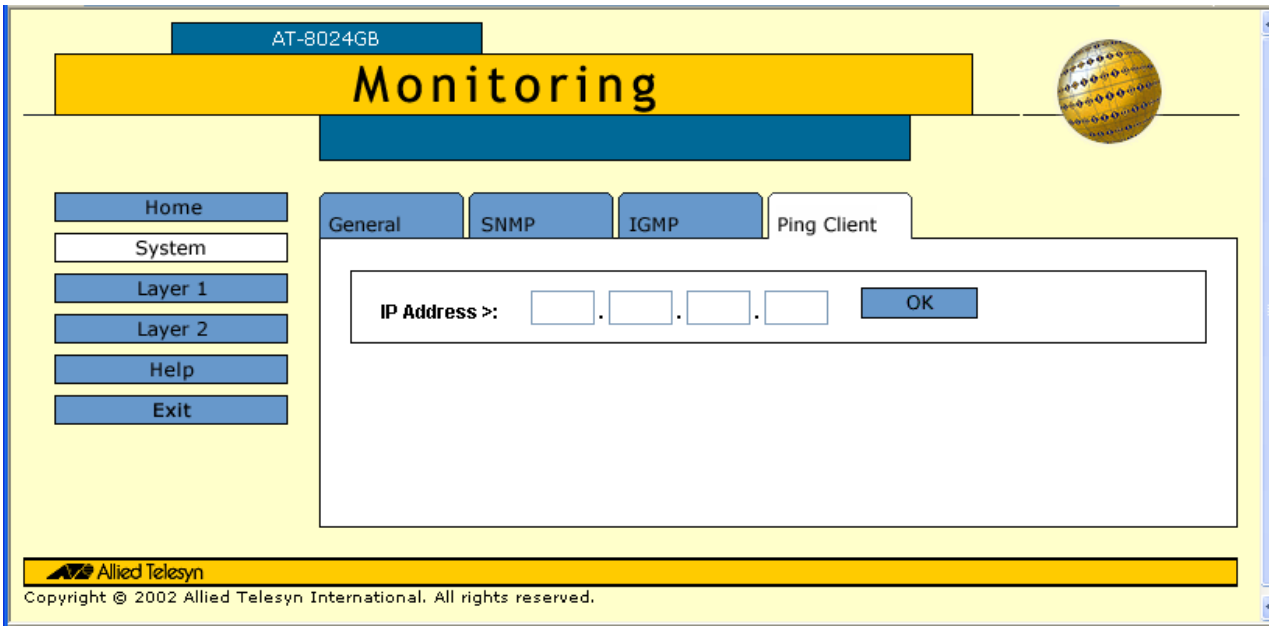

Figure 70 Ping Client Menu

4. Enter the IP address of the end node you want the switch to ping.
5. Click **OK**.

   The results of the ping are displayed in a new window.
6. To stop the pinging, click **OK**.

Returning the AT-S39 Software to the Factory Default Values

The procedure in this section returns all AT-S39 software parameters, except the IP address, subnet mask, and gateway address, to their default values. This procedure also deletes any VLANs that you have created on the switch.

> **Note**
> The AT-S39 software default values can be found in **Appendix A, AT-S39 Default Settings** on page 312.

To return the AT-S39 management software to its default settings, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **Factory Default** tab.

   The Factory Default tab in Figure 71 is displayed.

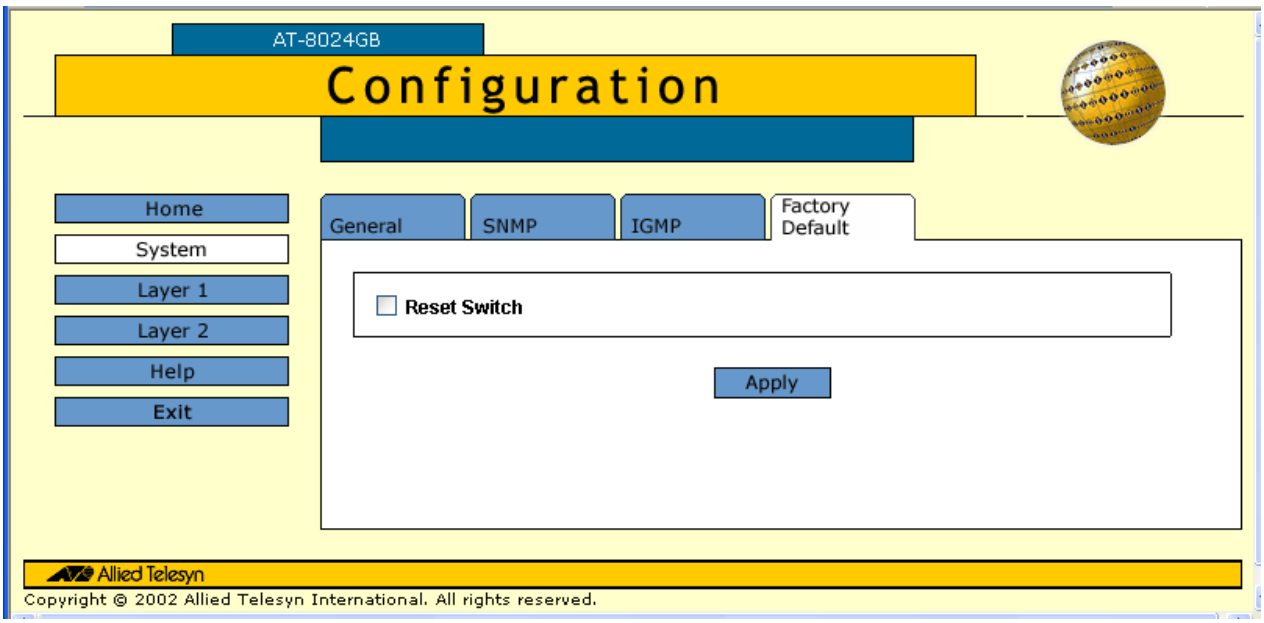

Figure 71 Factory Default Tab

4. Click the check box next to Reset Switch.
5. Click **Apply**.
6. Follow the prompts.

Chapter 23
Enhanced Stacking

This chapter contains the following procedures:

- **Setting a Switch's Enhanced Stacking Status** on page 245
- **Selecting a Switch in an Enhanced Stack** on page 247

Note
For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 58.

Note
Configuring Multiple VLANs on cascaded switches can affect Enhanced Stacking as the Master switch may not be able to detect member switches beyond the first cascaded switch.

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master, slave, or unavailable. Each status is described below:

- Master - A master switch of a stack can be used to manage all other AT-8000 Series switches in a subnet. Once you have established a local or remote management session with the master switch, you can access and manage all the switches in the subnet.

  A master switch must have a unique IP address. You can manually assign a master switch an IP address or activate the BOOTP and DHCP services on the switch.

- Slave - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask.

- Unavailable - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally. To be managed remotely, a switch with an unavailable stacking status must be assigned a unique IP address.

Note
The default setting for a switch is Slave.

To adjust a switch's enhanced stacking status, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. Select the **Enhanced Stacking** tab.

The Enhanced Stacking tab is shown in Figure 72.

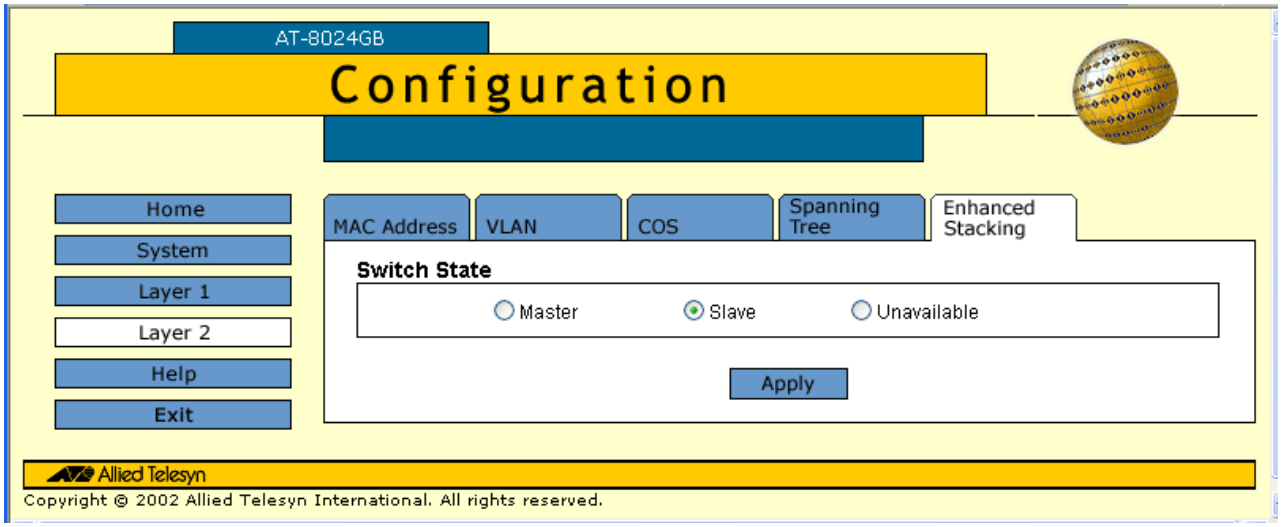

Figure 72 Enhanced Stacking Tab

4. Click the desired enhanced stacking status for the switch.
5. Click **Apply**.

   The new enhanced stacking status is immediately activated on the switch.

Selecting a Switch in an Enhanced Stack

The first thing that you should do before you perform any procedure on a switch in an enhanced stack is check to be sure that you are performing it on the correct switch. If you assigned system names to your switches, then it is very easy. The name of the switch being managed is displayed at the top of every management menu.

When you start a web browser management session on the master switch of a subnet, you are by default addressing that particular switch. The management tasks that you perform effect only the master switch.

To manage a slave switch or another master switch in the same subnet, you need to select it from the management software.

To select a switch to manage in an enhanced stack, perform the following procedure:

1. From the Home page, select **Enhanced Stacking**.

Note
If the Home page does not have an Enhanced Stacking menu selection, the switch's enhanced stacking status is either slave or unavailable. For instructions on how to change a switch's stacking status, refer to the previous procedure.

The master switch polls the network for all AT-8000 Series slave and master switches in the same subnet and displays a list of the switches in the Stacking Switches menu, shown in Figure 73.

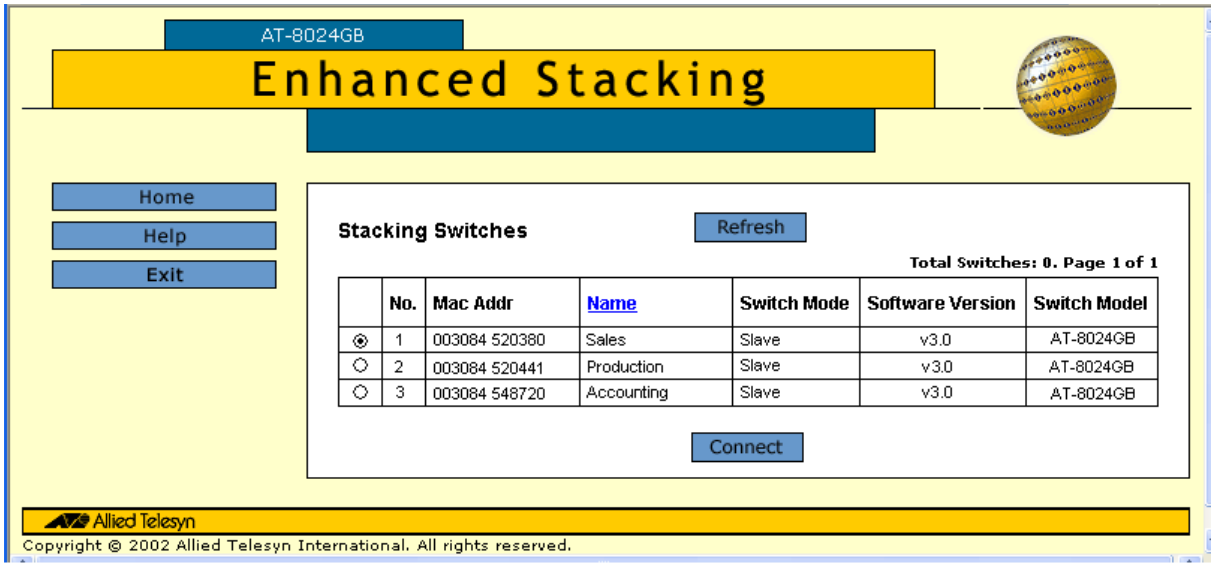

Figure 73 Stacking Switches Menu

Note
The master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of Unavailable.

You can sort the switches in the list by switch name or MAC address by clicking on the column headers. By default, the list is sorted by MAC address.

You can refresh the list by clicking **Refresh**. This instructs the master switch to again poll the subnet for all AT-8000 Series switches.

2. To manage another switch in an enhanced stack, click the dialog circle to the left of the appropriate switch in the list.
3. Click **Connect**.

   The Home page of the selected switch is displayed. You can now manage the switch.

Returning to the Master Switch

When you have finished managing a slave switch and want to manage another switch in the subnet, return to the Home page of the switch and select **Disconnect** from the menu. This returns you to the Stacking Switches window in Figure 73 on page 247. Once you see that window, you are again addressing the master switch from which you started the management session.

You can either select another switch in the list to manage or, if you want to manage the master switch, return to the master switch's Home page by selecting **Home**.

To end a management session, select **Exit**.

Chapter 24
Port Parameters

The procedures in this chapter allow you to view and change the parameter settings for the individual ports on a switch. Examples of port parameters that you can adjust include duplex mode and port speed.

This chapter contains the following procedures:

- **Configuring Port Parameters** on page 250
- **Displaying Port Status and Statistics** on page 253

Configuring Port Parameters

To configure the parameter settings for a port on a switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1**.
3. Select the **Port Setting** tab.

   The Port Setting tab is shown in Figure 74.

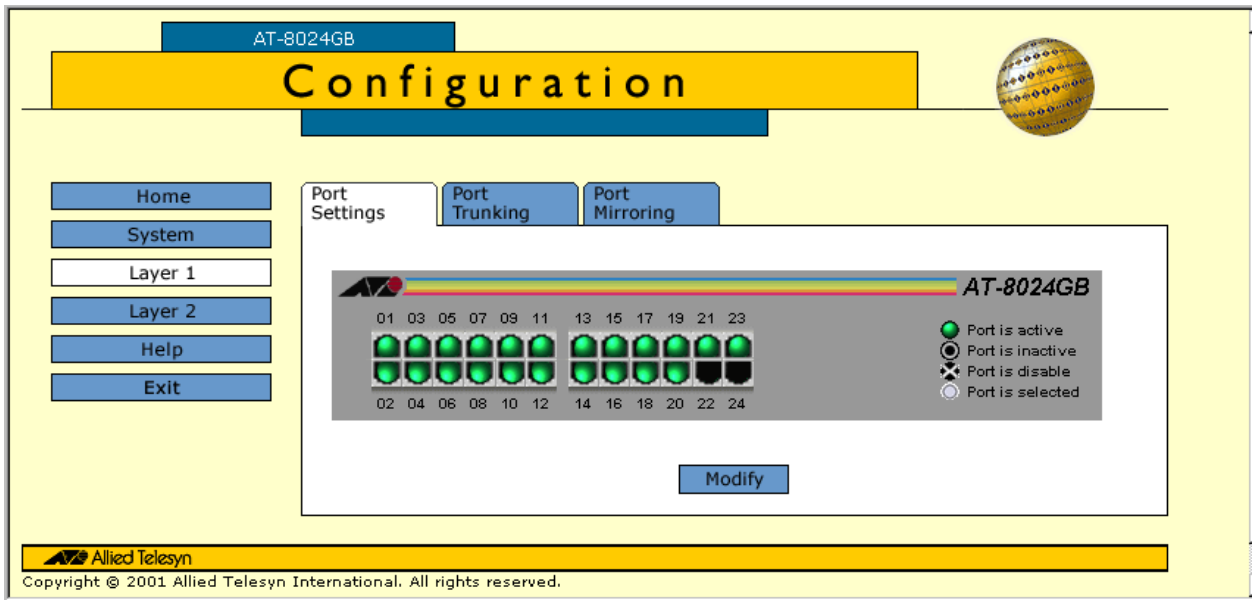

Figure 74 Port Setting Configuration Tab

4. Click the port in the graphical switch image that you want to configure. The selected port turns white. You can select more than one port at a time to configure. (To deselect a port, click it again.)
5. Click **Modify**.

The Settings for Port menu is displayed. An example of the menu is shown in Figure 75.

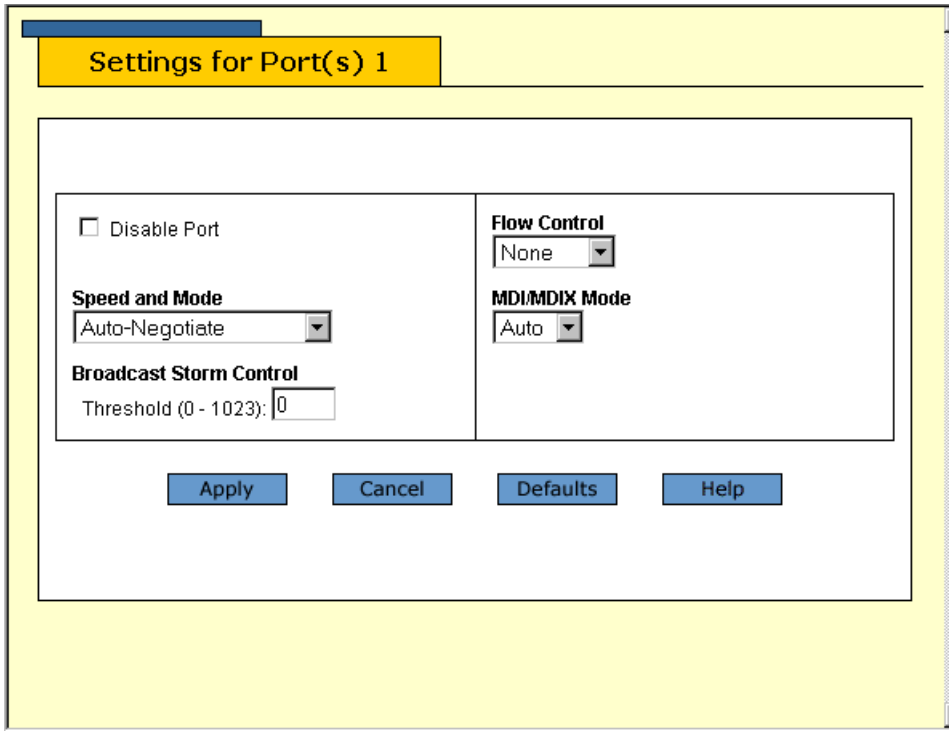

Figure 75 Settings for Port Menu

Note
Clicking the **Default** button returns the port settings to the default values. Default values are listed in **Appendix A, AT-S39 Default Settings** on page 312.

6. Adjust the port parameters as desired.

   The parameters are described below.

   Disable Port
   You can use this check box to enable or disable a port. A disabled port will not accept or transmit frames. The default for this port parameter is enabled.

   Speed and Mode
   The operating speed and duplex mode of the port. Possible settings for this parameter are:

   - Auto-Negotiate: The port will Auto-Negotiate both speed and duplex mode. This is the default.
   - 10Mbps - Half Duplex
   - 10Mbps - Full Duplex

- ❑ 100Mbps - Half Duplex
- ❑ 100Mbps - Full Duplex

Broadcast Storm Control
The maximum number of broadcast packets the port can receive within a specified period of time. If the threshold is reach, any additional broadcast packets received on the port are discarded by the switch. For background information on this feature, refer to **Broadcast Storm Control Overview** on page 186. For instructions on how to set this value, refer to **Setting the Maximum Number of Broadcast Frames** on page 306.

Flow Control
The flow control setting for the port. Possible values are:

None - No flow control on the port.

Transmit - Flow control only on packets being transmitted out of the port.

Receive - Flow control only on packets being received on the port.

Both - Flow control for both packets entering and leaving the port.

MDI/MDIX
The wiring configuration of the port. The default setting of Auto has the port configure itself automatically as MDI or MDIX, depending on the end node. You can use this option to configure a port's wiring configuration manually.

Note
The Auto setting is not available if you set a port's speed and duplex mode manually.

7. Once you have made the desired changes, click **Apply**.

   The switch immediately activates the parameter changes on the port.

Displaying Port Status and Statistics

The procedure in this section displays the operating status of the ports on a switch and port statistics. You can view a port's operating speed, duplex mode, MDI/MDI-X configuration, and more. You can also view the operating status of any GBIC modules installed in an AT-8024GB.

To display the status or statistics of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring page, select **Layer 1**.
3. Select the **Port Settings** tab. The tab is shown in Figure 76.

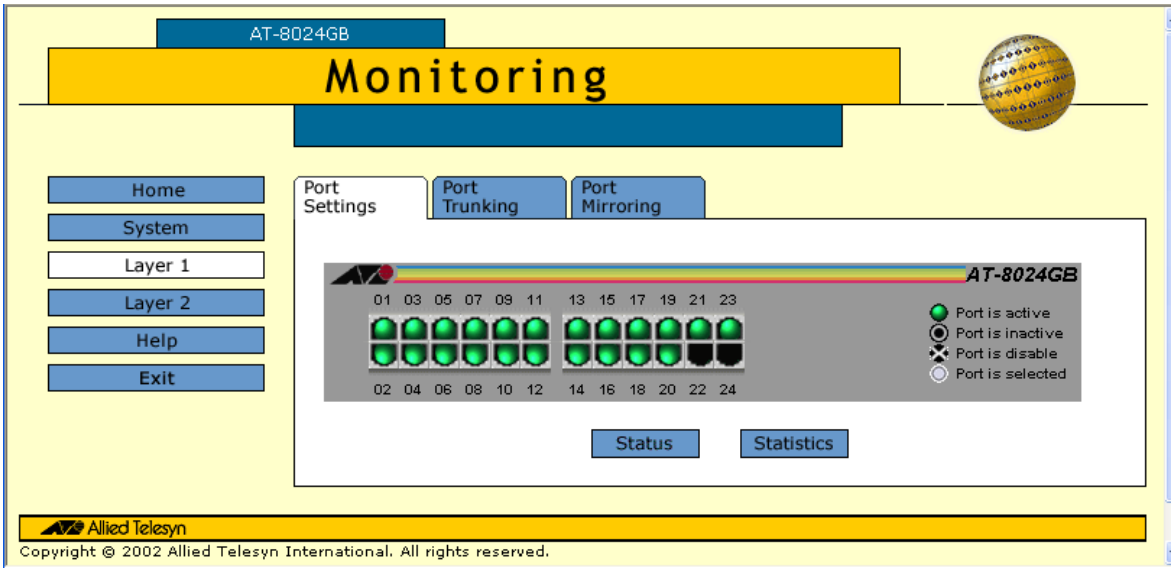

Figure 76 Port Monitoring Page

This page displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

4. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)
5. Click **Status** to display the port's operating status or **Statistics** to display port statistics.

If you select port status, the Port Status window in Figure 77 is displayed.

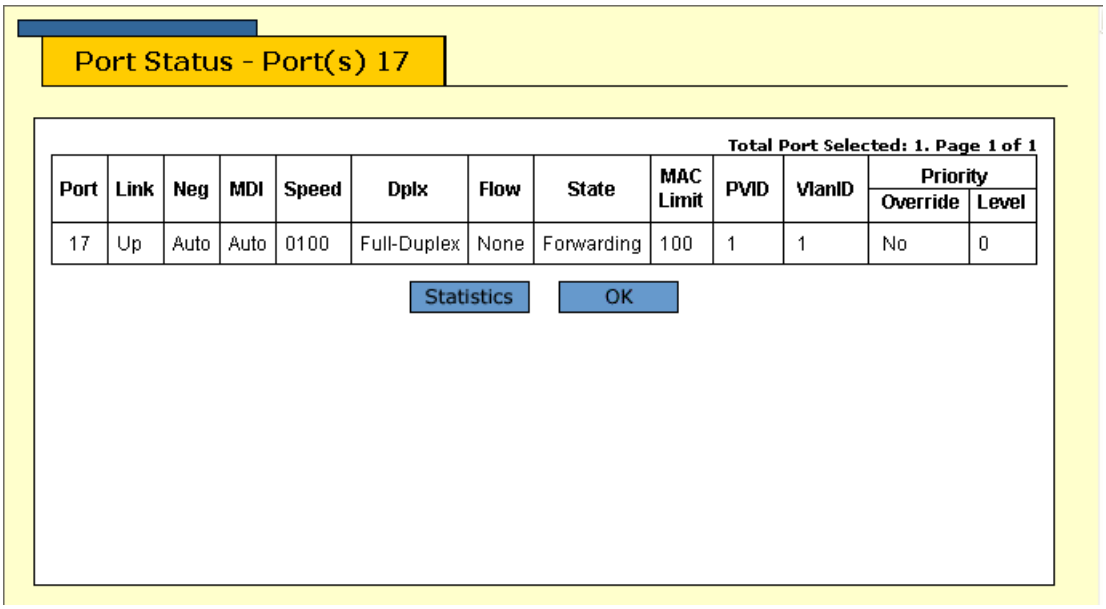

Figure 77 Port Status Window

The information in this window is for viewing purposes only. To adjust port parameters, refer to **Configuring Port Parameters** on page 250.

The columns in the window are described below:

Port
The port number.

Link
The status of the link between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Neg
The status of Auto-Negotiation on the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode.

Manual - Indicates that the operating speed and duplex mode are set manually.

MDI
The operating configuration of the port. Possible values are MDI and MDI-X.

Speed
The operating speed of the port. Possible values are:

0010 - 10 Mbps

0100 - 100 Mbps

1000 - 1000 Mbps

Dplx
The duplex mode of the port. Possible values are half-duplex and full-duplex.

Flow Control
The port's flow control setting. Possible values are:

None - No flow control on the port.

Transmit - Flow control only on packets being transmitted out the port.

Receive - Flow control only on packets being received on the port.

Both - Flow control for both packets entering and leaving the port.

State
The operating status of the port. Possible values are Forwarding and Disabled.

MAC Limit
The maximum number of MAC addresses the port can learn when operating in the Limited security mode. This value is only operational when the port is operating in the Limited security mode.

PVID
The port VLAN identifier assigned to the port.

VLAN
The VID of the VLAN in which the port is an untagged member.

Priority Override
The status of the override priority feature. If the status is Yes, tagged and untagged packets entering the port are directed to either to low or high priority queue as specified in CoS. If the status is No, tagged frames entering the port are directed to the low or high queue according to the priority levels specified in the tagged packets. For further information on this feature, refer to **Class of Service Overview on page 175**.

Priority Level
The priority queue to which untagged packets are directed when received on the port. A value of 1 to 3 directs untagged packets to the low priority queue while a value of 4 to 7 directs packets to the high priority queue. If the override priority feature has been activated on the port, tagged packets will be directed to the priority queue reflected by this status parameter. For further information on this feature, refer to **Class of Service Overview on page 175**.

If you select Statistics, the Statistics window in Figure 78 is displayed.

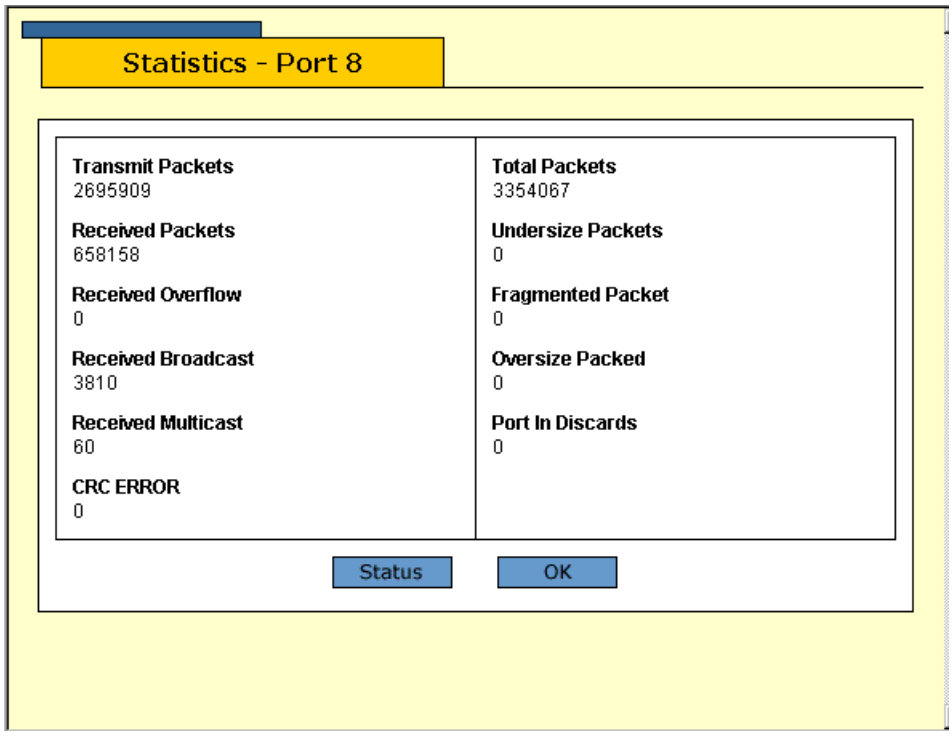

Figure 78 Port Statistics Window

The information in this window is for viewing purposes only. The statistics are defined below:

Transmit Packets
Number of packets transmitted out the port.

Received Packets
Number of packets received on the port.

Received Overflow
Number of times frames entering the port have exceeded the capacity of the port's buffer.

Received Broadcast
Number of broadcast packets received on the port.

Received Multicast
Number of multicast packets received on the port.

CRC Error
Number of packets with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port

Total Packets
Number of packets received and transmitted on the port.

Undersize Packets
Number of packets that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Fragmented Packets
Number of undersized packets, packets with alignment errors, and packets with FCS errors (CRC errors) received on the port.

Oversize Packets
Number of packets exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Port in Discards
Number of frames successfully received and buffered by the port, but discarded and not forwarded.

Chapter 25
Port Security

This chapter explains how to display the current port security level on the switch from a web browser management session.

Note
For background information on port security, refer to **Port Security Overview** on page 76.

Note
A switch's port security level can be changed only from a local management session.

Displaying the Port Security Level

To display the switch's port security level, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **Port Security** tab.

   The current security level is displayed.

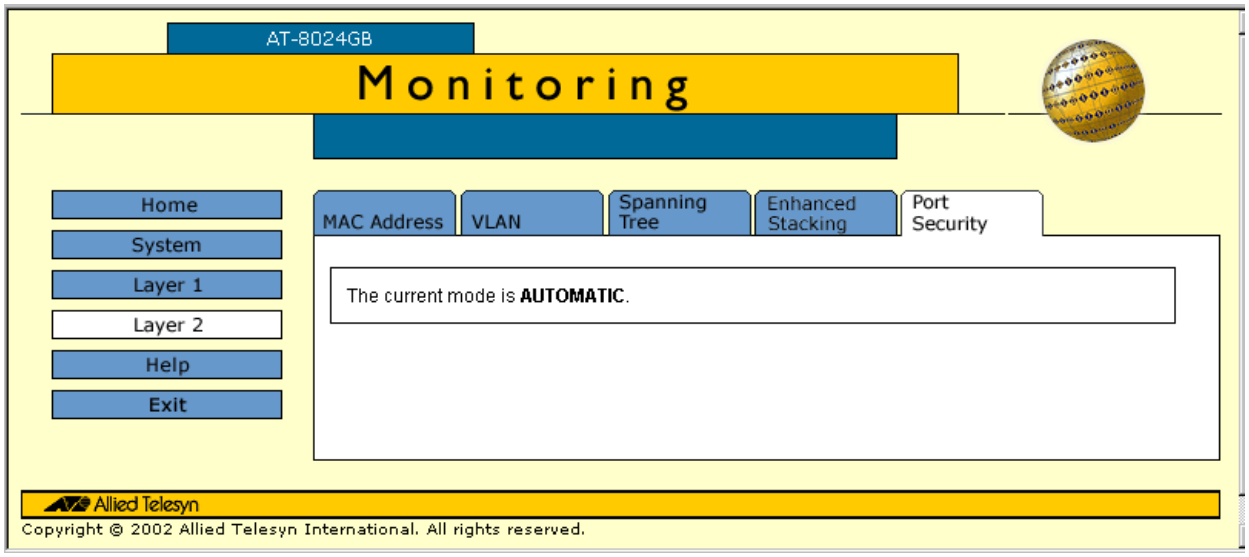

Figure 79 Port Security Menu

Chapter 26
Port Trunks

This chapter contains the procedure for creating or deleting a port trunk from a web browser management session.

Note
For background information on port trunking, refer to **Port Trunking Overview** on page 83.

Creating or Deleting a Port Trunk

Caution

Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms, which can adversely effect the operations of your network.

If you are deleting a port trunk, disconnect the cables from the ports before you delete the trunk. Deleting the trunk without first disconnecting the data cables can create a loop in your network topology, which can result in broadcast storms.

To create or delete a port trunk, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1**.
3. Select the **Port Trunking** tab.

   The management software displays the Port Trunking menu in Figure 80.

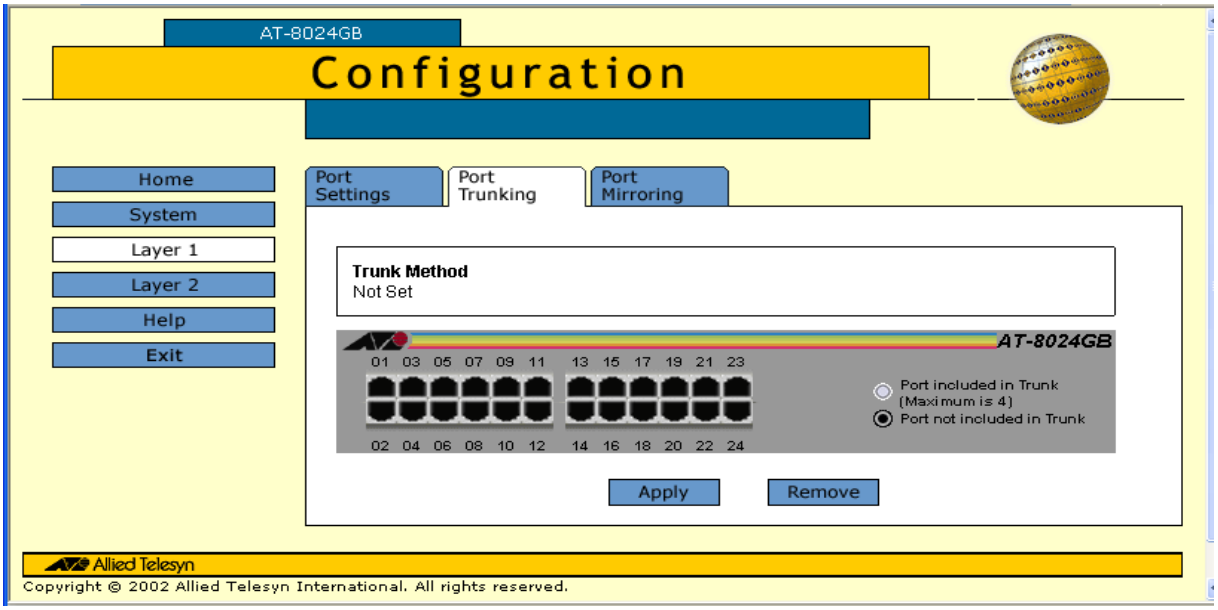

Figure 80 Port Trunking Menu

If the switch does not contain a port trunk, all ports in the switch image will be black. If there is a port trunk, the ports of the trunk will be white.

4. To create a port trunk, do the following:
   a. Click the ports that will make up the port trunk. A selected port changes to white. An unselected port is black. A port trunk can contain 2, 3, or 4 ports.
   b. Click **Apply**.

      Once you have selected the ports of the trunk, the following appear under Trunk Method.

   c. Click the desired load distribution method. The default is SA/DA.
   d. Configure the ports on the remote switch for port trunking.

   The new port trunk is immediately activated on the switch. You can now connect the data cables to the ports of the trunk on the switch.
5. To delete a port trunk, click **Remove**. The port trunk is immediately deleted from the switch.

Chapter 27
Port Mirroring

This chapter contains the procedure for creating or deleting a port mirror.

> **Note**
> For background information on port mirroring, refer to **Port Mirroring Overview** on page 93.

Creating or Deleting a Port Mirror

To create or delete a port mirror, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1**.
3. Select the **Port Mirroring** tab.

   The management software displays the Port Mirroring menu in Figure 81.

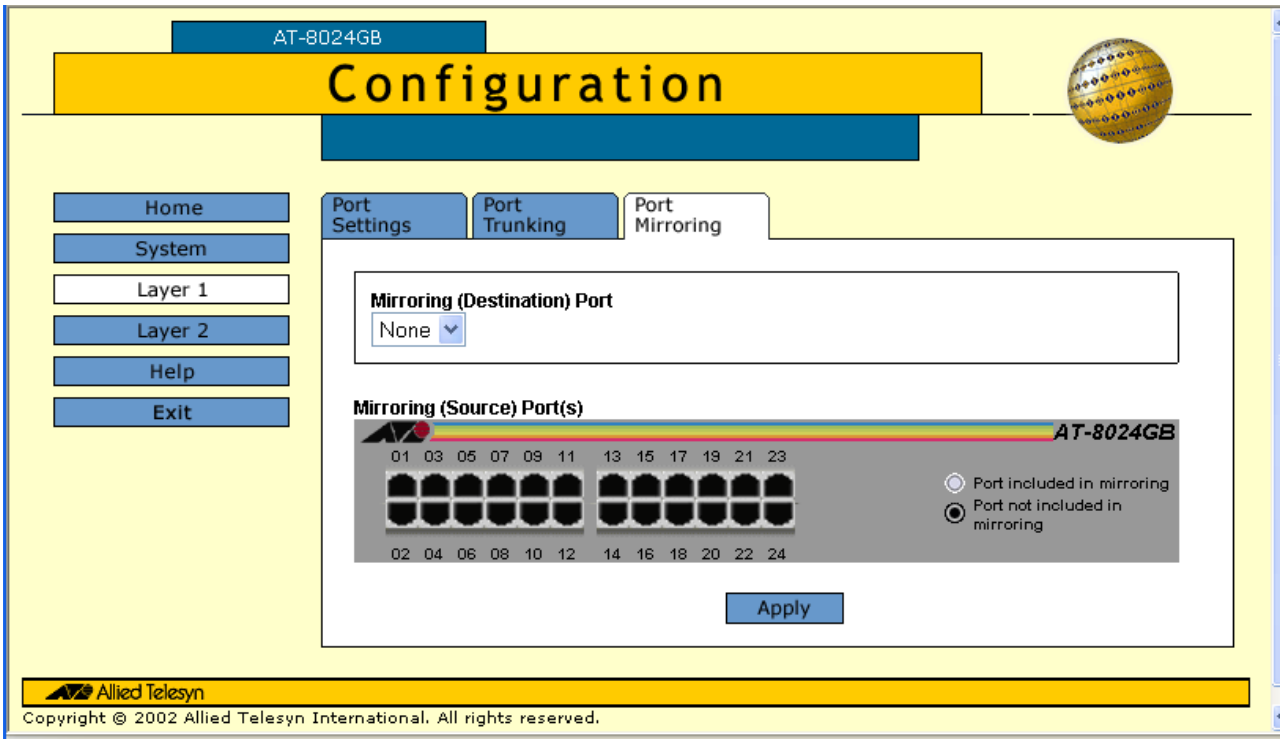

Figure 81 Port Mirroring Menu

4. To create a port mirror, do the following:

   a. Use the pull-down menu from Mirroring Port to select the port to function as the port mirror.

   b. Click the port(s) in the graphical switch image whose traffic is to be copied to the mirror port. You can select from 1 to 23 ports.

   c. Click **Apply**.

   The port mirror is immediately activated on the switch. You can now connect a data analyzer to the mirror port to monitor the traffic on the selected ports.

5. To disable port mirroring, select "None" from the Mirroring Port pull-down menu and click **Apply**.

   The port mirror is deleted. The port that was functioning as the mirror port can now be used for normal network operations.

Chapter 28
STP and RSTP

This chapter explains how to configure the STP and RSTP parameters on an AT-8000 Series switch from a web browser management session.

Sections in the chapter include:

- **Enabling or Disabling STP or RSTP** on page 267
- **Configuring STP** on page 268
- **Configuring RSTP** on page 272
- **Displaying STP or RSTP Settings** on page 276

Note
For background information on spanning tree, refer to **STP and RSTP Overview** on page 97.

Enabling or Disabling STP or RSTP

To enable or disable spanning tree on the bridge, do the following:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **Spanning Tree** tab.

   The Spanning Tree tab in Figure 82 is displayed.

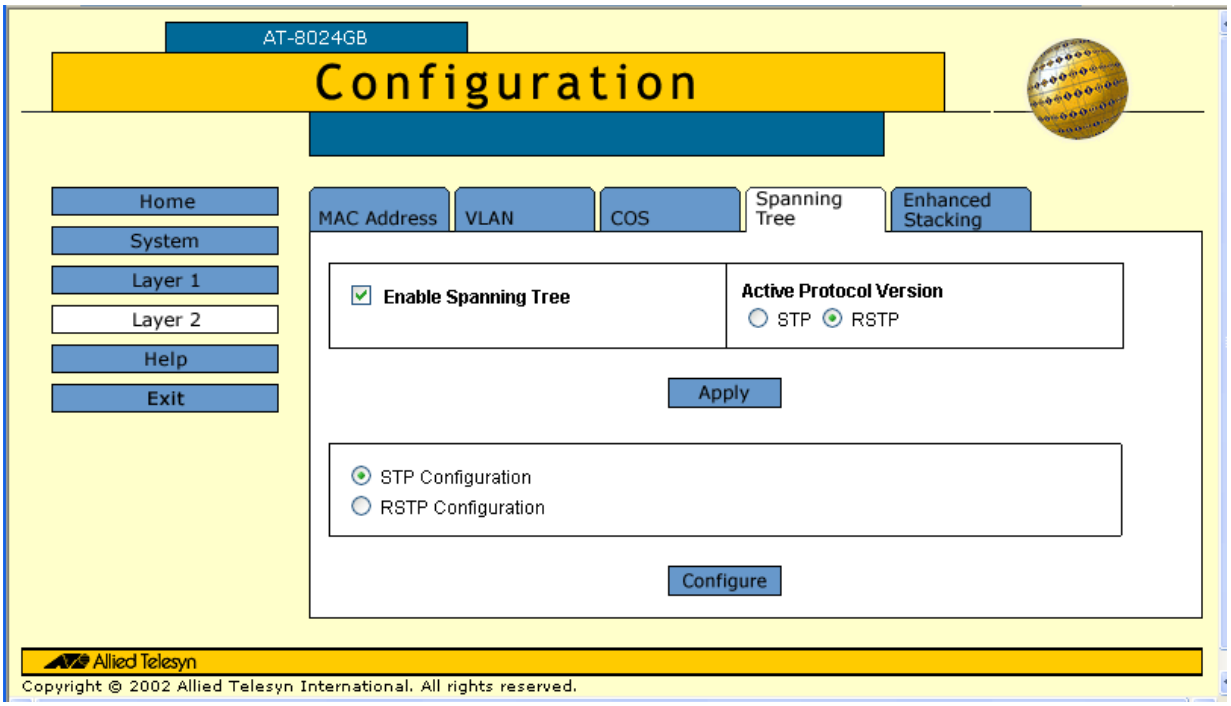

Figure 82 Spanning Tree Tab

4. To enable or disable spanning tree, click the **Enable Spanning Tree** check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.
5. If you are activating spanning tree, click either **STP** or **RSTP** in the Active Protocol Version section of the menu. The default is RSTP.

   Note
   Only one spanning tree protocol can be active on the switch at a time.

6. Click **Apply**.
7. If you activated STP, go to **Configuring STP** on page 268. If you activated RSTP go to Step **Configuring RSTP** on page 272.

Configuring STP

Caution
The bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

1. From the Spanning Tree tab menu, click STP Configuration and click **Configure**.

   The Spanning Tree menu in Figure 83 is displayed.

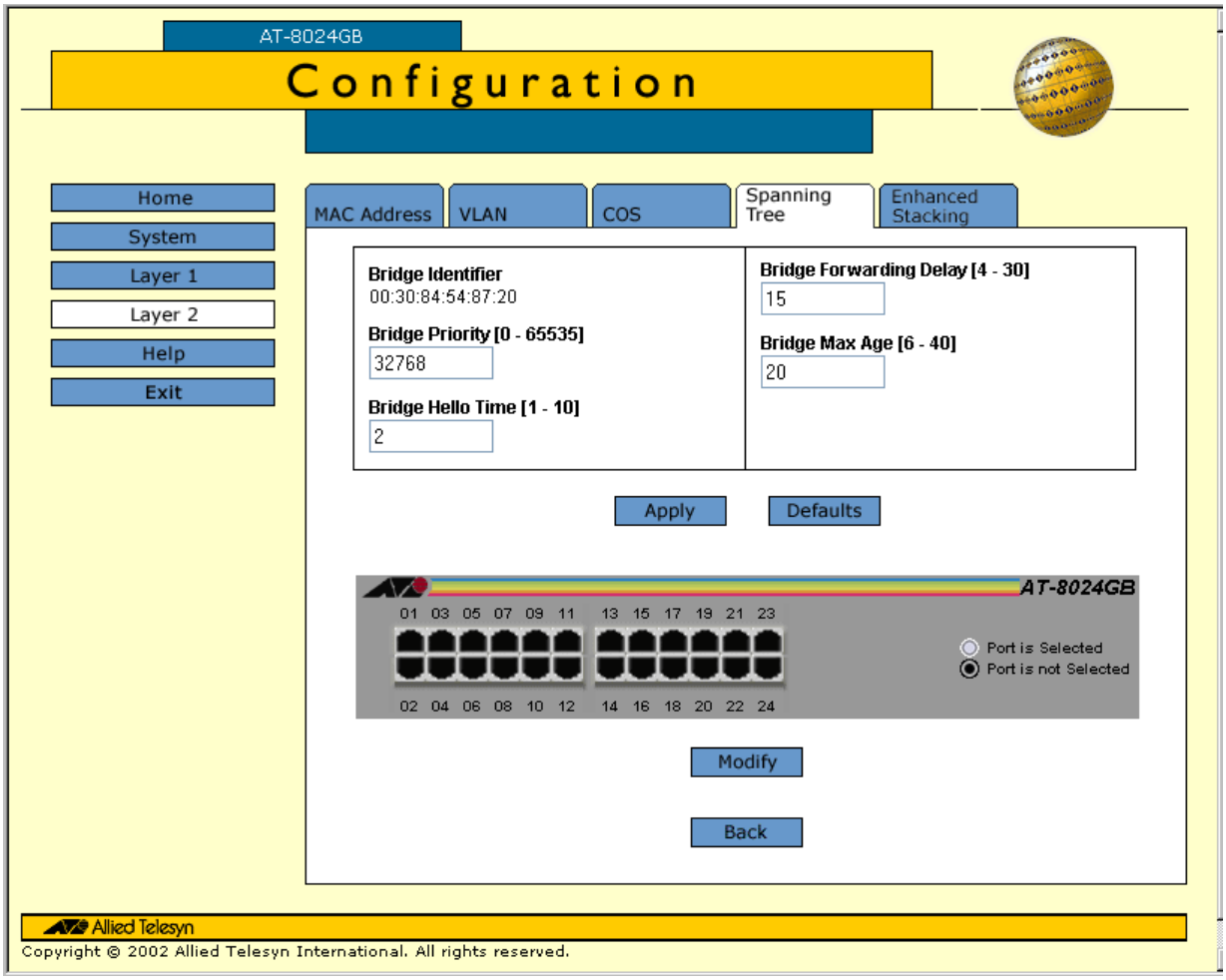

Figure 83 STP Bridge Configuration Menu

2. Adjust the bridge STP settings as needed. The parameters are described below.

   Bridge Identifier
   The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

   Bridge Priority
   The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 65,535, with 0 being the highest priority.

   Bridge Hello Time
   The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

   Bridge Forwarding Delay
   The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The default is 15 seconds.

   Bridge Max Age
   The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

   In selecting a value for maximum age, the following must be observed:

   MaxAge must be less then (2 x (HelloTime + 1)).

   MaxAge must be less then (2 x (ForwardingDelay - 1)).

Note
The aging time for BPDUs is different from the aging time used by the MAC address table.

3. After you have made the desired changes, click **Apply**.
4. To adjust a port's STP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

   The Port Spanning Tree Protocol menu in Figure 84 is displayed.

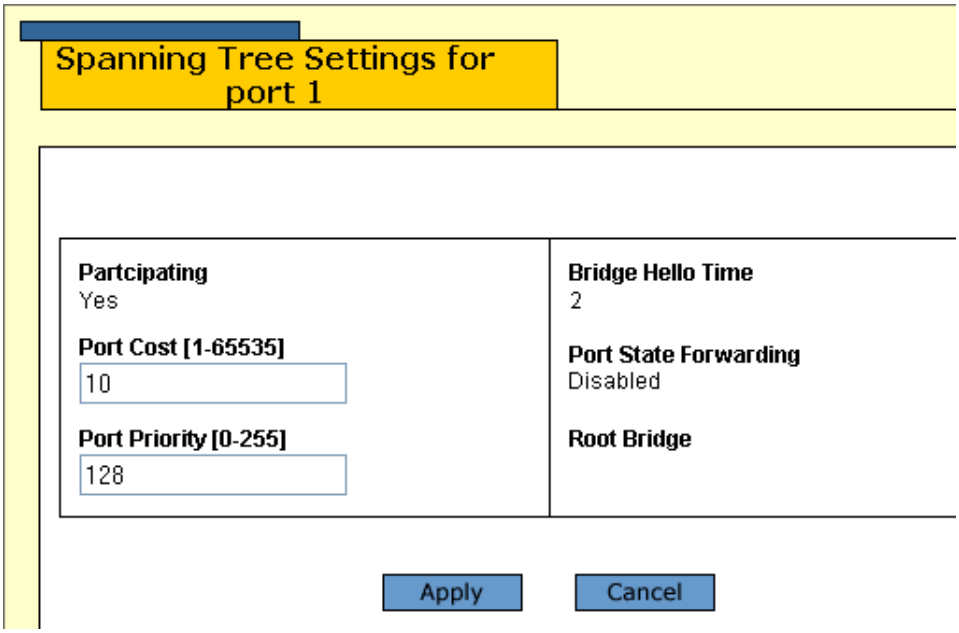

Figure 84 STP Port Configuration Menu

5. Adjust the settings as desired. The parameters are described below.

   Participating
   This parameter indicates whether the port is participating in the spanning tree domain. You cannot change this value from a web browser management session. It can be changed from a local or Telnet management session, as explained in **Configuring a Port's STP Settings** on page 108.

   Port Cost
   The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The default values for this parameter are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port. The range is 1 to 65535.

Port Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The default value for priority is 128. The range is 0-255.

Bridge Hello Time
The time interval between generating and sending configuration messages by the bridge. The default is 2 seconds. This value cannot be changed from this menu. To change this value, refer to earlier in this procedure.

Port State Forwarding
This field indicates whether the port is enabled or disabled.

Root Bridge
The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for display purposes only and cannot be changed.

6. Once you have configured the parameters, click **Apply**.

Note
A change to the port priority parameter takes effect immediately. A change to the port cost value requires youto reset the switch. A new port cost value is not implemented until the unit is reset.

Configuring RSTP

Caution
The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

1. From the Spanning Tree tab menu, click RSTP Configuration and click **Configure**.

The RSTP Bridge Configuration menu in Figure 83 is displayed.

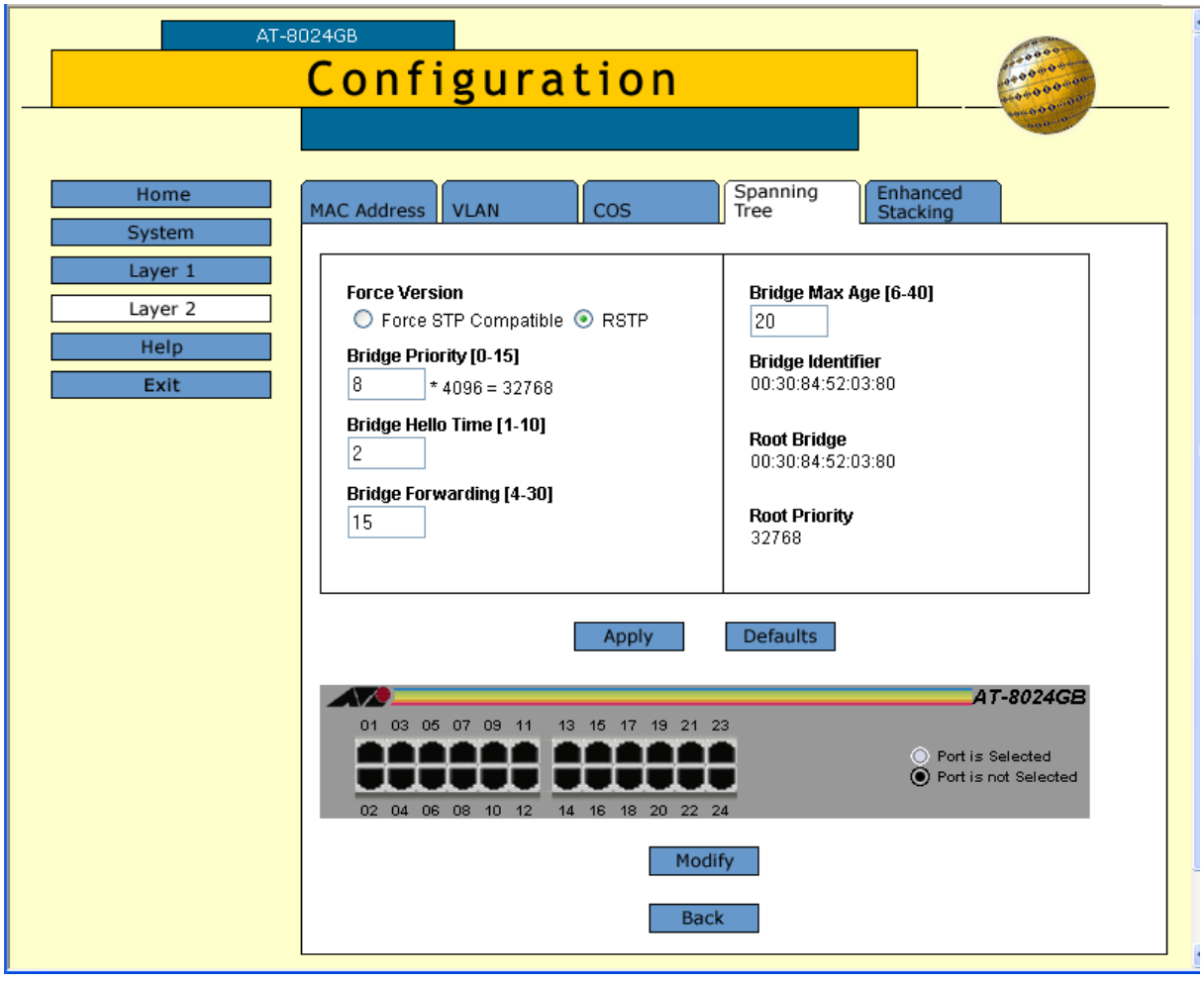

Figure 85 RSTP Bridge Configuration Menu

2. Adjust the parameters are desired. The parameters are defined below.

   Force Version
   This selection determines whether the bridge will operate with RSTP or in an STP-compatible mode. If you select RSPT, the bridge will operate all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge will operate all ports in STP. The default is RSTP.

   Bridge Priority
   The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to **Table 4**, **RSTP Bridge Priority Value Increments** on page 98

   Bridge Hello Time
   The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

   Bridge Forwarding
   The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds.

   Bridge Max Age
   The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

   In selecting a value for maximum age, the following must be observed:

   MaxAge must be less then (2 x (HelloTime + 1)).

   MaxAge must be less then (2 x (ForwardingDelay - 1)).

Bridge Identifier
The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

Root Bridge
The MAC address of the bridge functioning as the root bridge in the spanning tree domain. This value is for display purposes only and cannot be changed.

Root Priority
The priority number of the root bridge.

3. After you have made your changes, click **Apply**.
4. To adjust a port's RSTP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

   The Port Rapid Spanning Tree Protocol menu in Figure 86 is displayed.

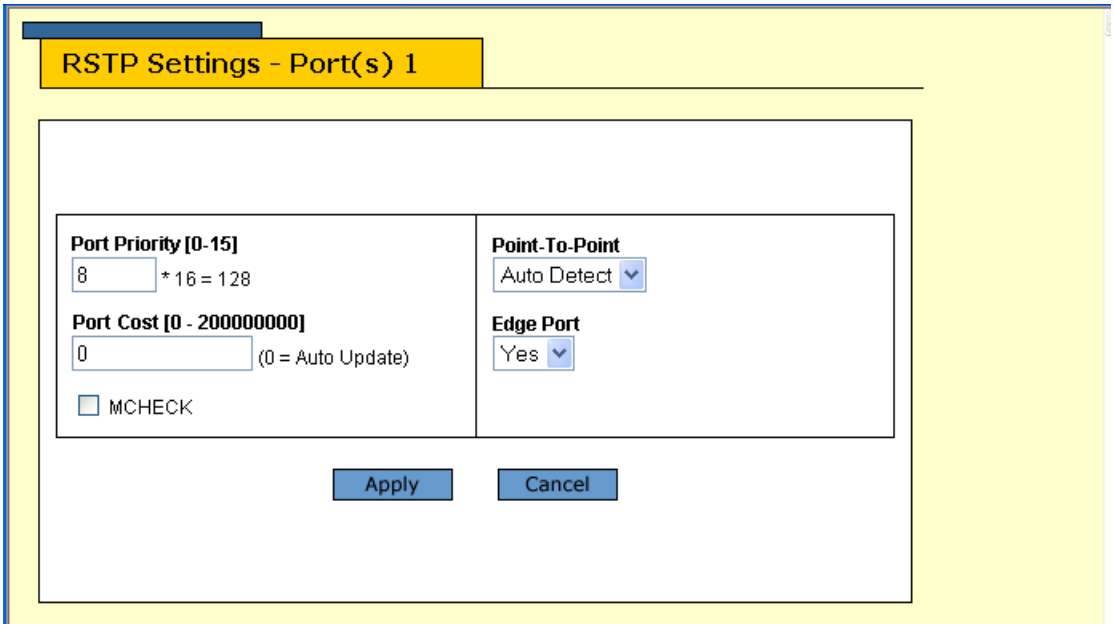

Figure 86 RSTP Port Configuration Menu

5. Adjust the settings as desired. The parameters are described below.

Port Priority
This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value of 128). For a list of the increments, refer to **Table 7**, **RSTP Port Priority Value Increments** on page 100.

Port Cost
The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20 000 000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port.

MCHECK
This option instructs the bridge to send out RSTP BPDU packets for several seconds from the selected port. The purpose is to determine if there are any RSTP or STP bridges connected to the port. If the port receives STP BPDU packets in response, the port changes to STP compatible mode.

Point-to-Point
This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 102.

Edge Port
This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 102.

6. Once you have configured the parameters, click **Apply**.

Note
All changes to a port's RSTP settings, with the exception of port cost, are activated immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Displaying STP or RSTP Settings

To display STP or RSTP parameter settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Layer 2**.
3. From the Layer 2 page, select the **Spanning Tree** tab.

   The Spanning Tree menu in Figure 88 is displayed. This menu displays information on whether spanning tree is enable or disabled and which protocol version, STP or RSTP, is active.

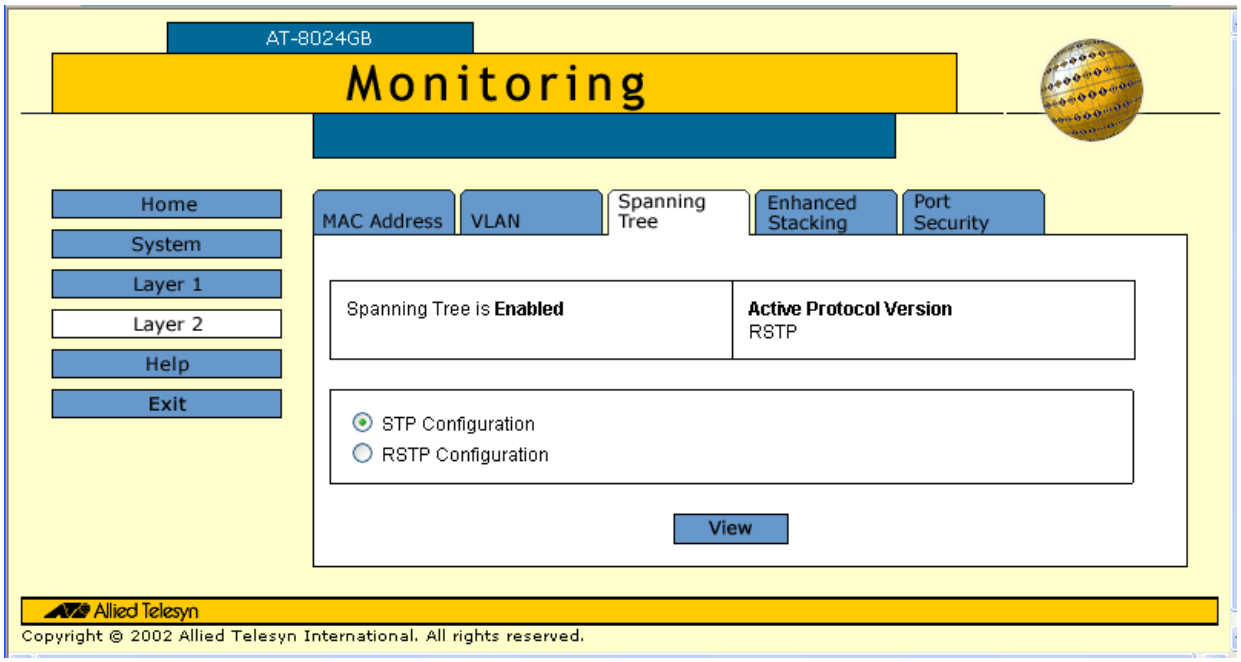

Figure 87 Spanning Tree Tab - Monitoring

4. To view STP or RSTP parameter settings, click either **STP Configuration** or **RSTP Configuration** and click **View**.

The example in Figure 88 is for RSTP. The information in this window is for viewing purposes only.

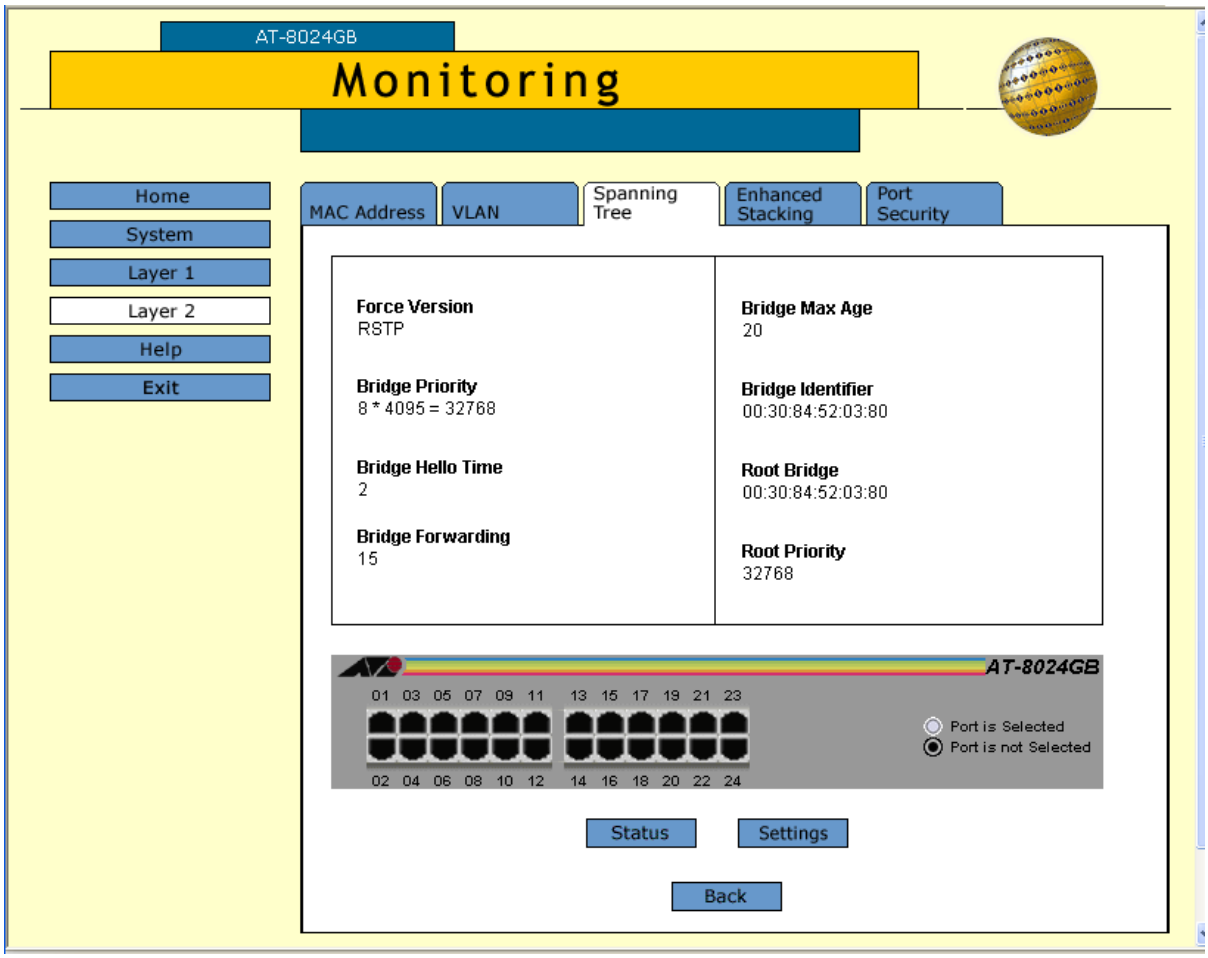

Figure 88 Rapid Spanning Tree Window - Monitoring

5. To view port settings, click a port in the switch and click **Status** or **Settings**.

Chapter 29
Virtual LANs

This chapter explains how to create, modify, and user-configured (port-based and tagged) and multiple VLANs in a web browser management session. This chapter also explains how to select a multiple VLANchange a switch's VLAN operating mode.

Note
For background information on switch modes and VLAN modes, refer to **Chapter 10, Virtual LANs**.

This chapter contains the following sections:

- ❑ **Creating A New Port-Based or Tagged VLAN** on page 279
- ❑ **Modifying a Port-Based or Tagged VLAN** on page 282
- ❑ **Deleting a Port-Based or Tagged VLAN** on page 283
- ❑ **Deleting a Port-Based or Tagged VLAN** on page 283
- ❑ **Displaying VLANs** on page 284
- ❑ **Selecting a Multiple VLANs Mode** on page 285
- ❑ **Setting the Switch's Mode** on page 287
- ❑ **Enabling or Disabling VLANs** on page 288

Creating A New Port-Based or Tagged VLAN

To create a new port-basedor tagged VLAN, perform the procedure below:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 89 is displayed.

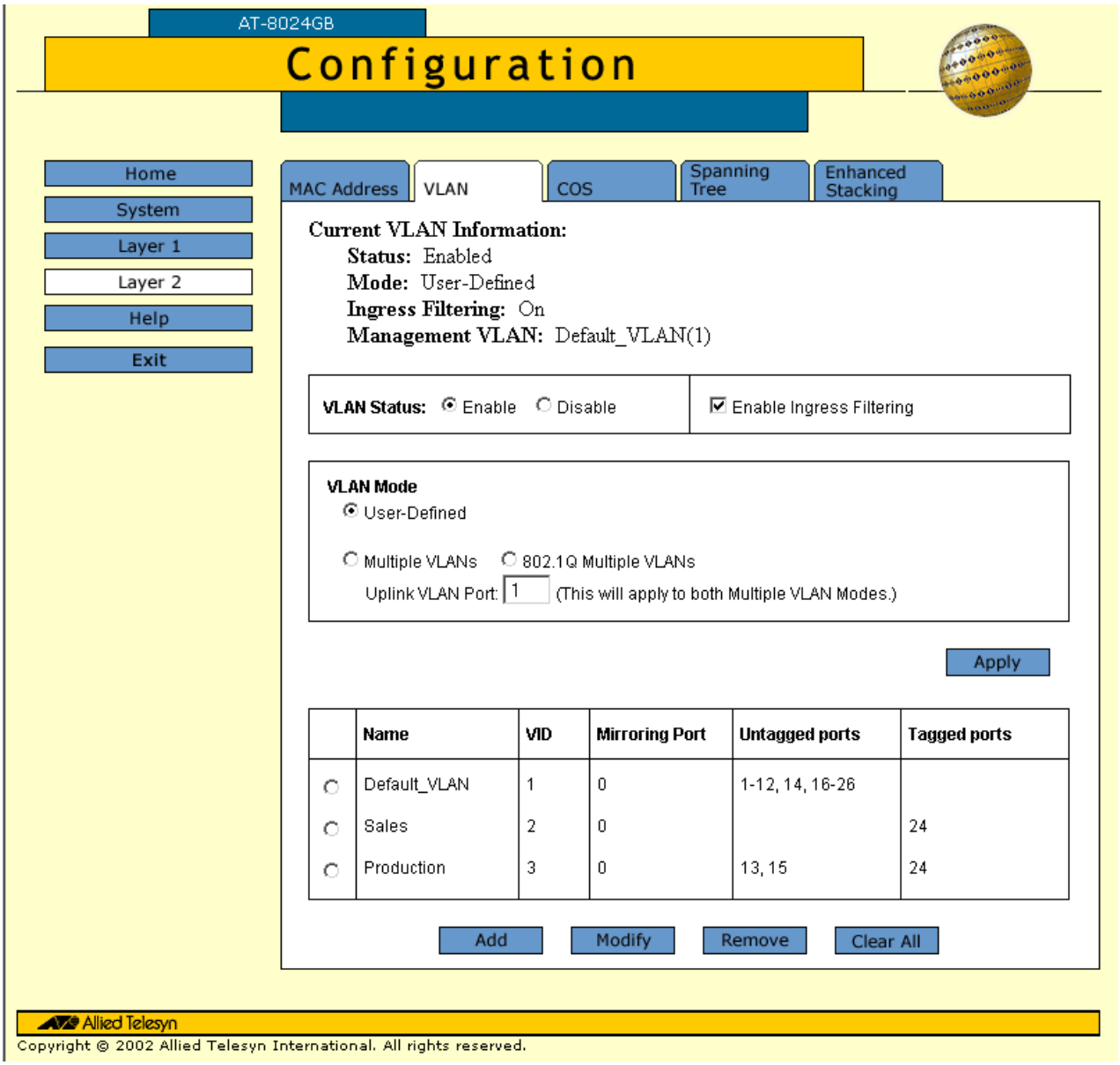

Figure 89 VLAN Menu

4. Click **Add**. The Add VLAN menu in Figure 90 is displayed.

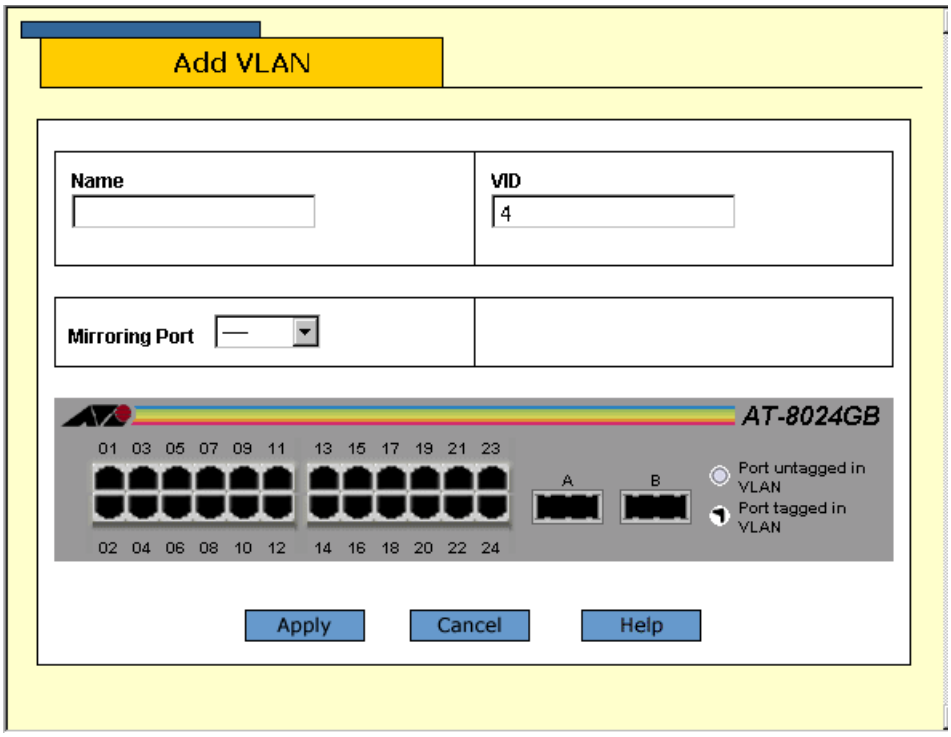

Figure 90 Add VLAN Menu

5. Select the **Name** field and enter a name for the new VLAN.

   The name can be from one to 10 characters in length. The name should reflect the function of the nodes of the VLAN (for example, Sales or Accounting). The name can contain spaces but not special characters, such as asterisks (*) or exclamation points (!).

   If the VLAN will be unique in your network, the name should be unique as well. If the VLAN will be part of a larger VLAN that spans multiple switches, the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

   Note
   A VLAN must be assigned a name.

6. Select the **VID** field and enter a VID value for the new VLAN. The range of the VID value is 2 to 4096. The default will be the next available VID number on the switch.

   If this will be a unique VLAN in your network, its VID must be unique as well. If the VLAN will be part of a larger VLAN that spans multiple switches, its VID value should be the same on each switch. For

example, if you are creating a VLAN called Sales that will span three switches, you must assign the same VID value to each Sales VLAN on the three switches.

Note
A VLAN must have a VID.

7. If you want all received traffic on the ports of the VLAN to be mirrored to another port on the switch, select the mirroring port from the **Mirroring Port** pull-down menu.

   This feature is useful when troubleshooting a VLAN. You can analyze the VLAN traffic by placing a network analyzer on the mirroring port.

   In most cases, you should not change this parameter's default value of "—". This value disables port mirroring.

   Note
   For background information on port mirroring, refer to **Port Mirroring Overview** on page 93.

8. To select ports for the VLAN, click on the appropriate ports in the switch image.

   Clicking repeatedly on a port toggles the port through the following possible settings:

   Untagged port

   Tagged port

   Port not a member of the VLAN

9. Click **Apply**.

   Note
   The untagged ports that you assign to the new VLAN are automatically removed from their current VLAN assignment.

   The user-configured VLAN is now ready for network operations. For additional information on user-configured VLANs, refer to **User-Configured VLANs** on page 121

Modifying a Port-Based or Tagged VLAN

To modify a VLAN, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 89 on page 279 is displayed.
4. Click the circle next to the name of the VLAN you want to modify.
5. Click **Modify**.

   The configuration menu for the VLAN is displayed.
6. Modify the VLAN parameters by referring to Step 5 to Step 8 in the previous procedure, **Creating A New Port-Based or Tagged VLAN** on page 279.

   When modifying a VLAN, observe the following guidelines:

   - ❑ You cannot change the VID of a VLAN.
   - ❑ You cannot change the name of the Default_VLAN.
   - ❑ When changing a VLAN's name or VID, be sure that the new name or VID is unique on the switch.
7. After making the desired changes, click **Apply**.

   Note
   Untagged ports that are added to a VLAN are automatically removed from their current VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

   Removing an untagged port from the Default_VLAN without assigning it to another VLAN will leave the port as an untagged member of no VLAN.

   The modified VLAN is now ready for network operations.

Deleting a Port-Based or Tagged VLAN

To delete a VLAN from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 89 on page 279 is displayed.
4. Click the circle next to the name of the VLAN you want to delete.
5. Click **Remove**.

   A confirmation prompt is displayed.
6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure.

   If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.

Note
You cannot delete the Default_VLAN.

To delete all VLANs from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 89 on page 279 is displayed.
4. Click **Clear All**.

   A confirmation prompt is displayed.
5. Click **OK** to delete all the VLANs or **Cancel** to cancel the procedure.

   If you click OK, all VLANs except for the Default_VLAN are deleted from the switch. The ports in the VLANs are returned to the Default_VLAN as untagged ports.

Displaying VLANs

To display all the existing VLANs on a switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring page, select **Layer 2**.
3. From the Layer 2 page, select the **VLAN** tab.

   The management software displays the window in Figure 91. The information in this window is for viewing purposes only.

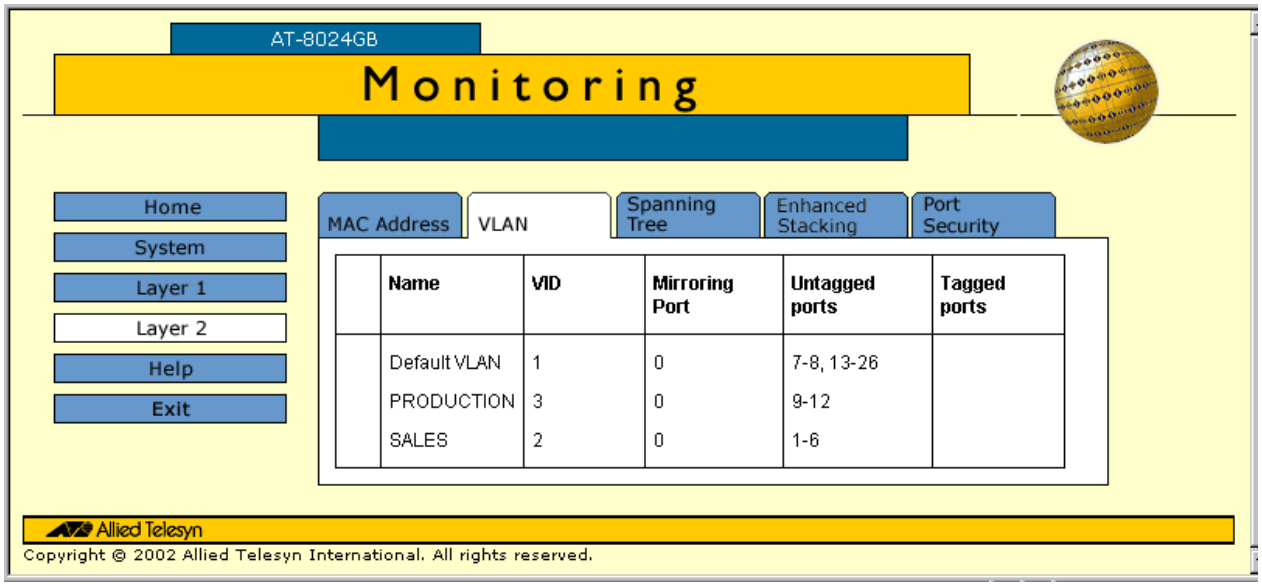

Figure 91 VLAN Monitoring Window

Selecting a Multiple VLANs Mode

To select a multiple VLAN mode, perform the procedure below:

> **Note**
> In 802.1Q Multiple VLANs mode, any device connected to the Uplink VLAN must be 802.1Q-compliant.

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab. The VLAN menu in Figure 89 is displayed.

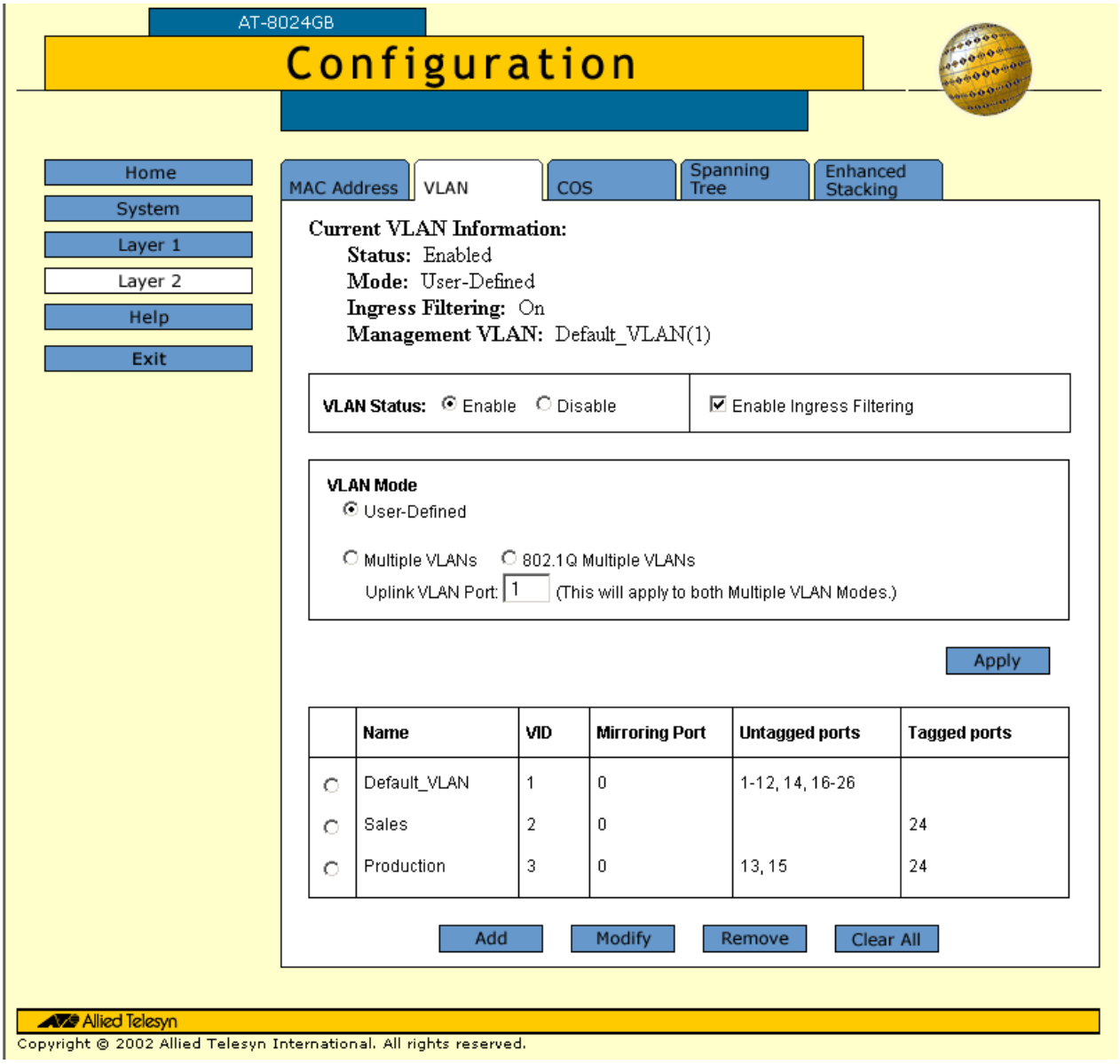

Figure 92 Multiple VLAN Configuration

4. Under VLAN Mode, select the non-802.1Q compliant **Multiple VLANs** or **802.1Q Multiple VLANs**.
5. In the Uplink VLAN Port field (under VLAN Mode), specify the port on the switch that will function as the uplink port for the VLANs.
6. Click **Apply**.
7. Reset the switch. For instructions, refer to **Resetting a Switch** on page 241.

For information on the difference between Multiple VLANs or 802.1Q Multiple VLANs, refer to **Multiple VLAN Mode Overview** on page 132.

Setting the Switch's Mode

This section contains the procedure for setting a switch's mode. You can configure a switch to Tagged mode or Basic mode.

> **Note**
> For descriptions of switch modes and VLAN modes, refer to **Virtual LANs Overview** on page 115.

To set the switch's VLAN mode, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. From the Configuration menu, choose **System**.
3. Select the **General** tab.
4. In the Switch Mode section of the menu, click either **Tagged** or **Basic**.

   If you select Tagged, which is the default, the switch will support both port-based VLANs and tagged VLANs. If you select Basic, the switch will operate in the Basic mode.
5. Click **Apply**.
6. Click **Reset** to reset the switch.

   A change to VLAN status is not activated until the switch is reset.

Enabling or Disabling VLANs

This procedure performs exactly the same function as the previous procedure. It sets a switch's VLAN mode. When VLANs are enabled, the switch supports port-based and tagged VLANs. When VLANs are disabled, the switch supports the Basic mode.

The difference between the two procedures has to do with ingress filtering. If you activate the Basic Mode using the previous procedure, ingress filtering is disabled. Performing this procedure does not change the current setting of ingress filtering.

To configure a switch's VLAN mode, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **Layer 2**.
3. From the Layer 2 window, select the **VLAN** tab.

   The VLAN menu in Figure 89 on page 279 is displayed.
4. Click the **Enable VLAN** check box. A check in the box indicates that the switch supports tagged and untagged VLANs. No check in the box indicates that the switch is operating in the Basic Mode.
5. Click **Apply**.
6. Reset the switch. For instructions, refer to **Resetting a Switch** on page 241. A change to VLAN status is not activated until the switch is reset.

Chapter 30
MAC Address Table

This chapter contains instructions on how to view the dynamic and static addresses in the MAC address table of the switch. This chapter contains the following procedure:

- ❑ **Viewing the MAC Address Table** on page 290
- ❑ **Adding Static and Multicast MAC Addresses** on page 293
- ❑ **Deleting MAC Addresses** on page 294
- ❑ **Changing the Aging Time** on page 295

Note
For background information on MAC addresses, refer to **MAC Address Overview** on page 162.

Viewing the MAC Address Table

To view the MAC address table, perform the following procedure:

1. From the Home page, select either **Configuration** or **Monitoring**.
2. Select **Layer 2**.
3. From the Layer 2 page, select the **MAC Address** tab.

   The MAC Address menu is displayed. Figure 93 shows how this menu appears when you display it through the Configuration main menu selection. If displayed through the Monitoring main menu selection, the Add button is not included. This button is used to add static and multicast address to the switch. For instructions on how to add static and multicast MAC addresses, refer to the next procedure.)

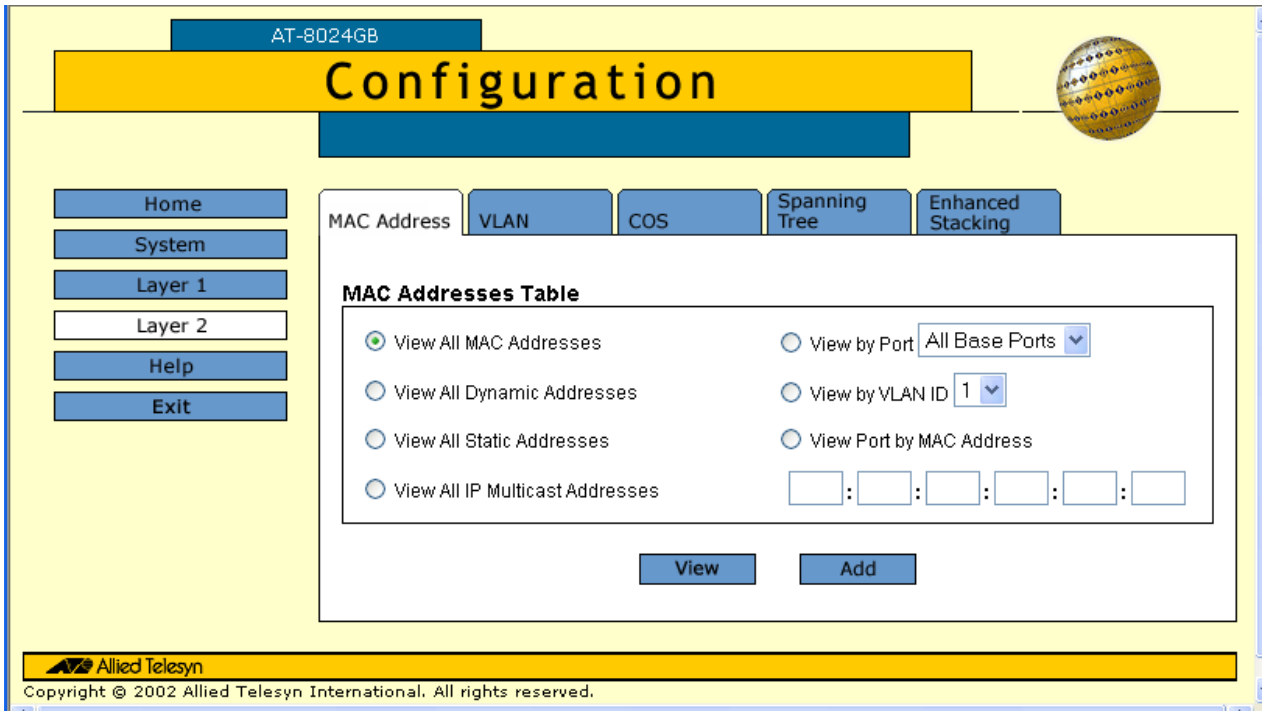

Figure 93 Forwarding Database Tab

The options for displaying MAC addresses are described below.

View All MAC Addresses
This option displays both static and dynamic MAC addresses.

View All Dynamic Addresses
This option displays only dynamic MAC address. Dynamic MAC addresses are addresses that the switch has learned by examining the source addresses of frames received on the ports.

View All Static Addresses
This option displays only the static MAC addresses. Static MAC addresses are addresses that you entered manually into the MAC address table.

View All IP Multicast Addresses
This option displays the multicast MAC addresses.

View By Port
The pull-down menu with this option is used to display the MAC addresses learned on a particular port.

View By VLAN ID
This option displays the MAC addresses learned by a particular VLAN on the switch. You specify the VLAN by its VID.

View Port by MAC Address
This option is used to determine the port on the switch to which an end node is communicating with the switch. To use this option, enter the MAC address of the node in the field.

4. Once you have selected one of the options, click **View**.

   The MAC addresses are displayed in a window. The columns in the window are defined below:

   MAC
   The MAC address of the node connected to the switch.

   Port
   The port on the switch where the MAC address was learned.

   PMAP
   The ports on the switch that are members of a multicast group. This column is useful in determining which ports belong to different multicast groups. It maps ports to multicast groups. (The abbreviation PMAP is derived from "port mapping.")

   Each "0" is a hexadecimal value for the binary value "0000". Each binary "0" represents a port on the switch. A binary "0" means that the port is not a member of a multicast group while a "1" means that it is.

   The port numbering scheme is from right to left. As an example, assume that ports 1 through 4 on the switch were members of the same multicast group. The PMAP column for the address would represent this as follows: "0000000F". Another example is "000020F. This example would indicate that ports 1 to 4 and port 10 on the switch were members of the same multicast group.

   CPU
   Indicates whether the traffic received on the port is sent to the switch's CPU. Yes indicates that the traffic is being sent to the CPU while No indicates it is not.

MIR
Indicates whether the traffic on the port is being mirrored. Yes means the traffic is being mirrored while No indicates that it is not.

EMP
Indicates whether multicast packets are being forwarded by ports in the blocking state. This feature is not supported at this time. This column will indicate “No” for all multicast addresses, except for the switch’s MAC address. Multicast packets are forwarded only by ports in the forwarding state.

VLANID
The VID of the VLAN to which the port is an untagged member.

Type
The MAC address type. The type can be either static or dynamic.

Adding Static and Multicast MAC Addresses

This section contains the procedure for assigning static or multicast address to ports on the switch. You can assign up to 255 static MAC addresses per port.

To add a static or multicast address to the MAC address table, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **MAC Address** tab.

   The MAC Address menu in Figure 93 on page 290 is displayed.
4. Click **Add**.

   The menu in Figure 94 is displayed.

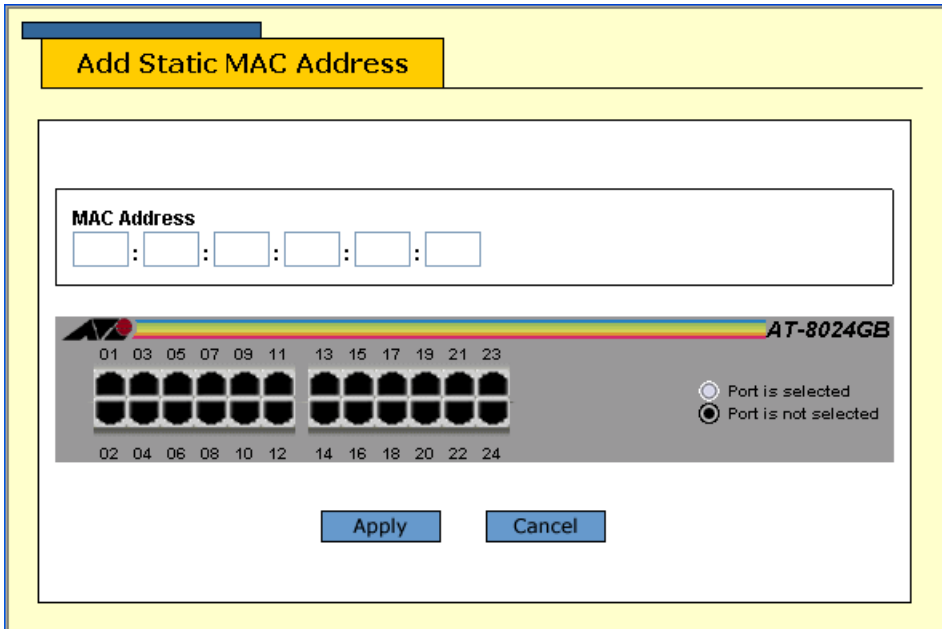
Add Static MAC Address
MAC Address
AT-8024GB
01 03 05 07 09 11 13 15 17 19 21 23
02 04 06 08 10 12 14 16 18 20 22 24
Port is selected
Port is not selected
Apply
Cancel

Figure 94 Add Static MAC Address Menu

5. In the MAC Address section of the menu, enter the new static or multicast MAC address.
6. In the graphical image of the switch click the port to which you want to assign the address. A selected port turns white. You can select only one port.
7. Click **Apply**.
8. Repeat this procedure to add other static or multicast addresses to the switch.

Deleting MAC Addresses

To delete a static, dynamic, or multicast MAC address from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **MAC Address** tab.

   The MAC Address menu in Figure 93 on page 290 is displayed.
4. Display the MAC addresses on the switch by selecting one of the options. For instructions, refer to **Viewing the MAC Address Table** on page 290.
5. Click on the dialog circle next to the MAC address that you want deleted from the switch.
6. Click **Remove**.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default setting for the aging time is 300 seconds (5 minutes).

To adjust the aging time, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **System**.
3. From the System page, select the **General** tab.

   The General tab in Figure 67 on page 233 is displayed.
4. Enter a new value in seconds in the MAC Aging Time field of the menu.

   The value should be an increment of 5 seconds, for example 410, 415, or 420. A value that is not an increment of 5 is rounded down to the next increment of 5. For example, the value 524 is rounded down to 520. The default is 300 seconds (5 minutes).
5. Click **Apply**.

Chapter 31
Class of Service

This chapter contains instructions on how to configure CoS. This chapter contains the following procedure:

- **Configuring CoS** on page 297

Note
For background information on CoS, refer to **Class of Service Overview** on page 175.

Configuring CoS

To configure CoS, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **CoS** tab.

   A graphical image of the switch is displayed.
4. Click the port where you want to configure CoS. You can select only one port at a time. A selected port turns white. (To deselect a port, click it again.)
5. Click **Modify**.

   The CoS Settings menu is displayed.
6. If you want all tagged and untagged frames received on the port to go to the low priority queue, select any level from Level 0 to Level 3 from the Priority pull-down menu. (It does not matter which of these levels you select.) If you want all frames received on the port to go to the high priority queue, select any level from Level 4 to Level 7. (Again, it does not matter which level you select.)
7. If you are configuring a tagged port and you want the switch to ignore the priority tag in the tagged frames entering the port, click the Override Priority option.

   All tagged frames will be directed to either the low or high priority queue specified in Step 5.

   Note
   The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame exits the switch with the same priority level that it had when it entered.

   The default for this parameter is No, meaning that the priority level of tagged frames is determined by the priority level specified in the frame itself.
8. Click Apply.

   Configuration changes are immediately activated on the switch.

Chapter 32
IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch.

> **Note**
> For background information on this feature, refer to **IGMP Snooping Overview** on page 178.

Sections in the chapter include:

- **Configuring IGMP Snooping** on page 299
- **Displaying a List of Host Nodes and Multicast Routers** on page 302

Configuring IGMP Snooping

To configure IGMP snooping from a web browser management session, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration menu, select **System**.
3. Select the **IGMP** tab.

   The IGMP tab in Figure 95 is displayed.

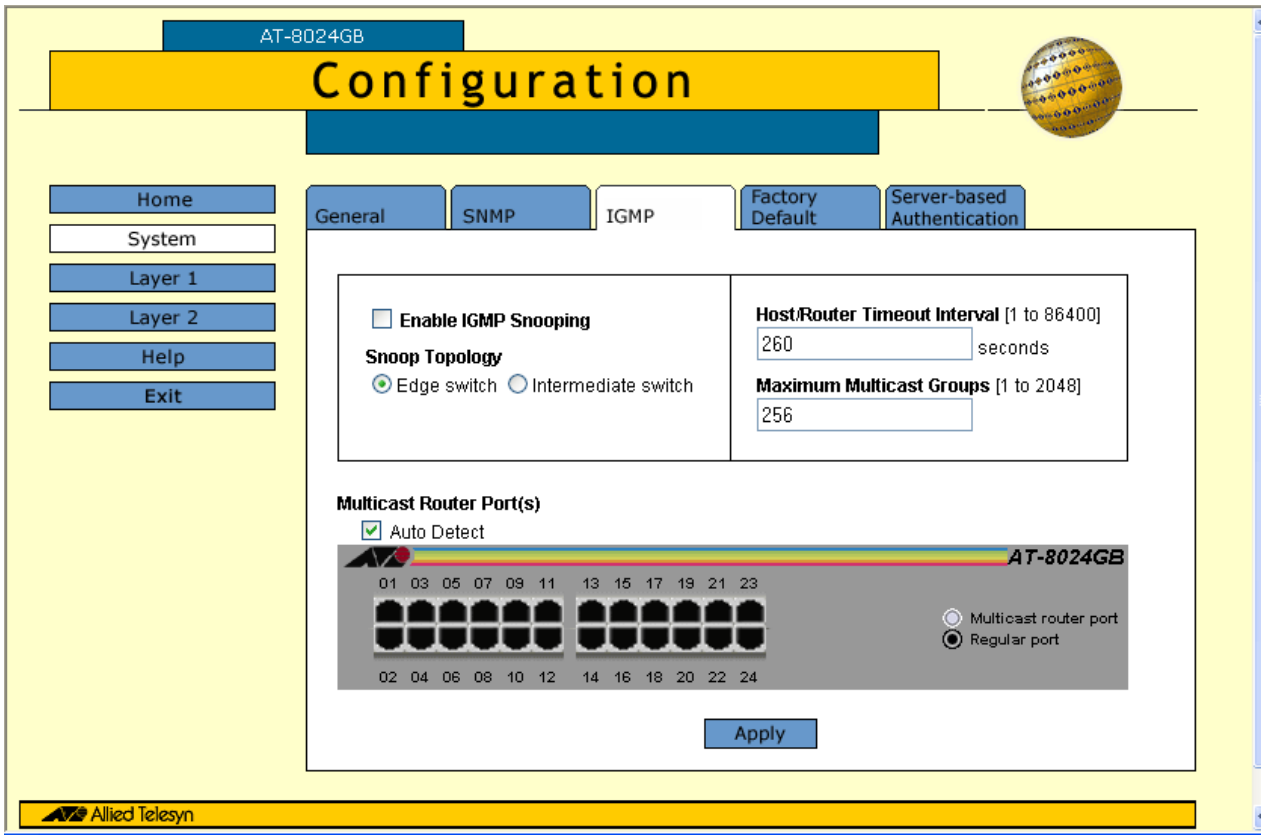

Figure 95 IGMP Menu - Configuration

4. Adjust the IGMP parameters as necessary.

   The parameters are explained below:

   Enable IGMP Snooping Status
   Enables and disables IGMP snooping on the switch. A check in the box indicates that IGMP is enabled.

Snoop Topology
Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

The Edge (Single-Host/Port) setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending reports and times-out. The switch forwards the leave request to the router and simultaneously ceases transmission of any further multicast packets out the port where the host node is connected.

The Intermediate (Multi-Host) setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port will continue to receive the multicast packets. Only after all of the host nodes connected to a switch port have transmitted leave requests (or have timed out) will the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Intermediate Multi-Host Port selection.

Host/Router Timeout Interval
Specifies the time period in seconds after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

Maximum Multicast Groups
Specifies the maximum number of multicast groups the switch will learn. The range is 1 to 2048 groups. The default is 256 multicast groups.

This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

Multicast Router Port(s)
Specifies the port on the switch to which the multicast router is detected. You can let the switch determine this automatically by selecting Auto Detect, or you can specify the port yourself by clicking on the ports in the graphical image. A white port indicates a multicast router port.

5. If desired, you can use the graphical image in the menu to indicate which ports on the switch are connected to multicast routers.

   By default, the switch automatically detects the presence of multicast routers by watching for queries on its ports. Once it has received a query, it notes the port on which the query was received and identifies the port as a multicast port.

   If desired, you can deactivate the auto-detection of multicast routers and indicate the multicast router ports yourself. To deactivate the auto-detection, click on the **Auto Detect** check box. If the check box is empty, auto-detect is deactivated.

   To indicate the multicast router ports manually, use the graphical image of the switch. Clicking a port toggles it to white, indicating that the port is connected to a multicast router.

6. After setting the IGMP parameters, click **Apply**.

Displaying a List of Host Nodes and Multicast Routers

You can use the AT-S39 software to display a list of the multicast groups on a switch, as well as the host nodes. You can also view the multicast routers. A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. To view host nodes and multicast routers, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring window, select the **System** menu option.
3. Select the **IGMP** tab.

   The window in Figure 96 is displayed.

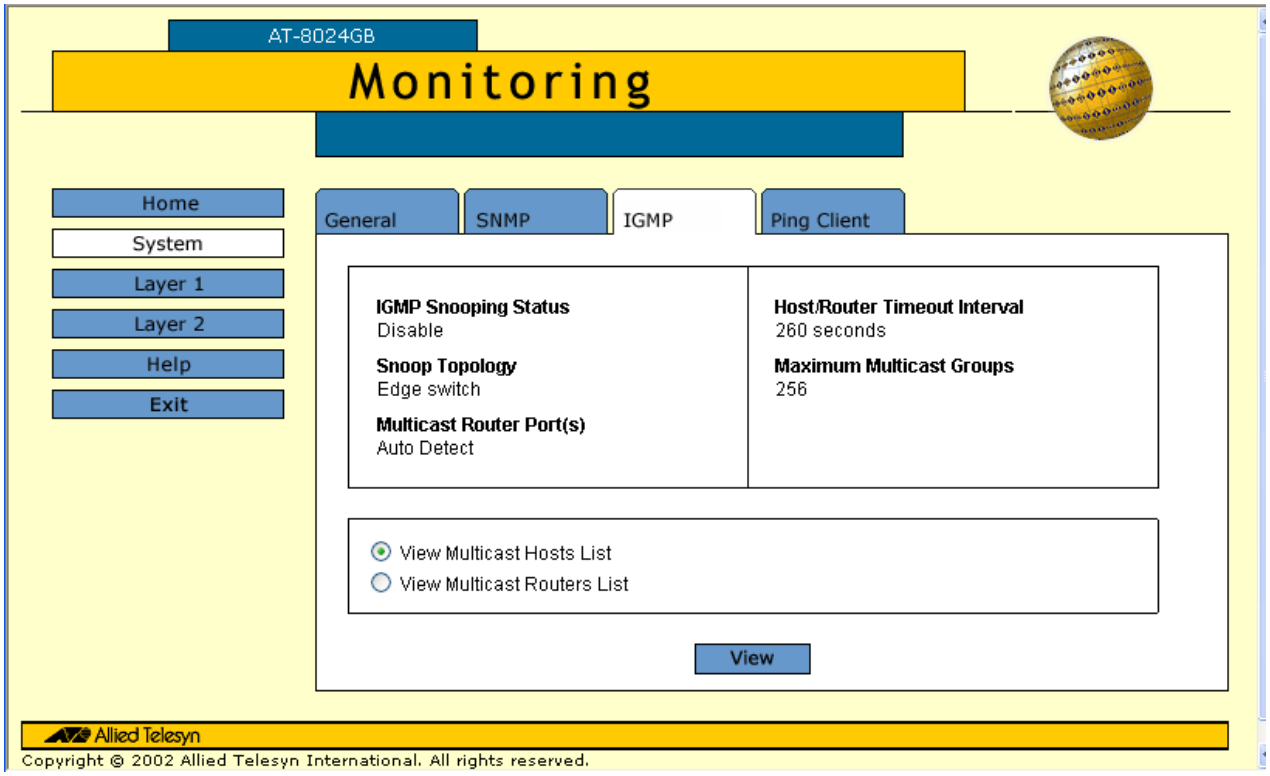

Figure 96 IGMP Window - Monitoring

4. To view the multicast addresses and the host nodes, click **View Multicast Host List** and then click **View**. To view the multicast routers, click **View Multicast Router List** and then click **View**.

Viewing a list of host nodes displays a window containing the following information. The information in the window is for viewing purposes only.

Multicast Group
The multicast address of the group.

Member Port
The port(s) on the switch to which one or more host nodes of the multicast group are connected.

VLAN ID
The VID of the VLAN in which the port is an untagged member.

Host IP
The IP address(es) of the host node(s) connected to the port.

Viewing a list of multicast routers displays a window containing the following information. The information in the window is for viewing purposes only.

Port
The port on the switch where the multicast router is connected.

VLAN ID
The VID of the VLAN in which the port is an untagged member.

Router IP
The IP address of the port on the router.

Chapter 33
Broadcast Storm Control

This chapter contains instructions on how to configure the Broadcast Storm Control feature on the switch.

Note
For background information on this feature, refer to **Broadcast Storm Control Overview** on page 186.

Configuring the Interval Timer

The interval timer defines the time period used in counting the number of broadcast packets transmitted by a port. A port will not transmit more than its maximum number of broadcast frames during the specified timer interval. If a port reaches its maximum number, it will discard and not forward any additional broadcast frames. You can specify a different interval timer for 10 and 100 Mbps ports and 1000 Mbps ports.

To specify an interval timer, perform the following procedure:

1. From the Home page, select **Configuration**.

   The System menu option is selected by default along with the General tab when you open the Configuration page. If they are not already selected, select them now.

2. In the Broadcast Storm Control section, enter values for the two interval timers.

   The interval timer for 10 Mbps and 100 Mbps ports is in milliseconds and has a range of 10 to 120 milliseconds. The value should be entered in increments of 10.

   The interval timer for 1000 Mbps ports is in microseconds and has a range of 100 to 120000 microseconds. The value should be entered in increments of 100.

   A value for an interval timer applies to all ports operating at the corresponding speed.

3. After you have entered your values, click **Apply**.

4. Go to the next procedure to set values for the maximum number of broadcast frames the ports on the switch will transmit.

Setting the Maximum Number of Broadcast Frames

To set the maximum number of broadcast frames you want the ports on the switch to transmit, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1**.

   When you open the Layer 1 page, the Port Settings tab is selected by default. If it is not selected, select it now.
3. In the graphical switch image, click a port where you want to specify the maximum number of broadcast frames.

   The selected port turns white. To deselect a port, click it again. You can select only one port at a time.
4. Click **Modify**.

   The current settings for the port are displayed in the Port Configuration menu.
5. In the Broadcast Storm Control section of the menu, enter the maximum number of broadcast packets you want the port to be able to transmit.

   The range is 0 to 1023 broadcast frames. Specifying a value of “0” disables Broadcast Storm Control on the port. The port will forward all broadcast frames.

   As an example, assume that you enter a value of 300 as the maximum number of broadcast frames for a port. Also assume that the port is operating at 100 Mbps and that you specified an interval timer of 100 milliseconds for 100 Mbps ports. The result would be that the port could transmit up to 300 broadcast frames every 100 milliseconds. If it received more than 300 broadcast frames for transmission during a 100 millisecond period, the extra broadcast frames would be discarded by the port and would not forwarded.
6. Click **Apply**.
7. Repeat this procedure to set the maximum number of broadcast frames for other ports on the switch.

Chapter 34
TACACS+ and RADIUS Protocols

This chapter contains instructions on how to configure the authentication protocols. This chapter contains the following procedure:

- **Configuring TACACS+ and RADIUS** on page 308

Note
For background information on the authentication protocols, refer to **TACACS+ and RADIUS Overview** on page 192.

Configuring TACACS+ and RADIUS

To configure the authentication protocols, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **System**.
3. From the System page, select the **Server-based Authentication** tab. The tab is shown in Figure 97.

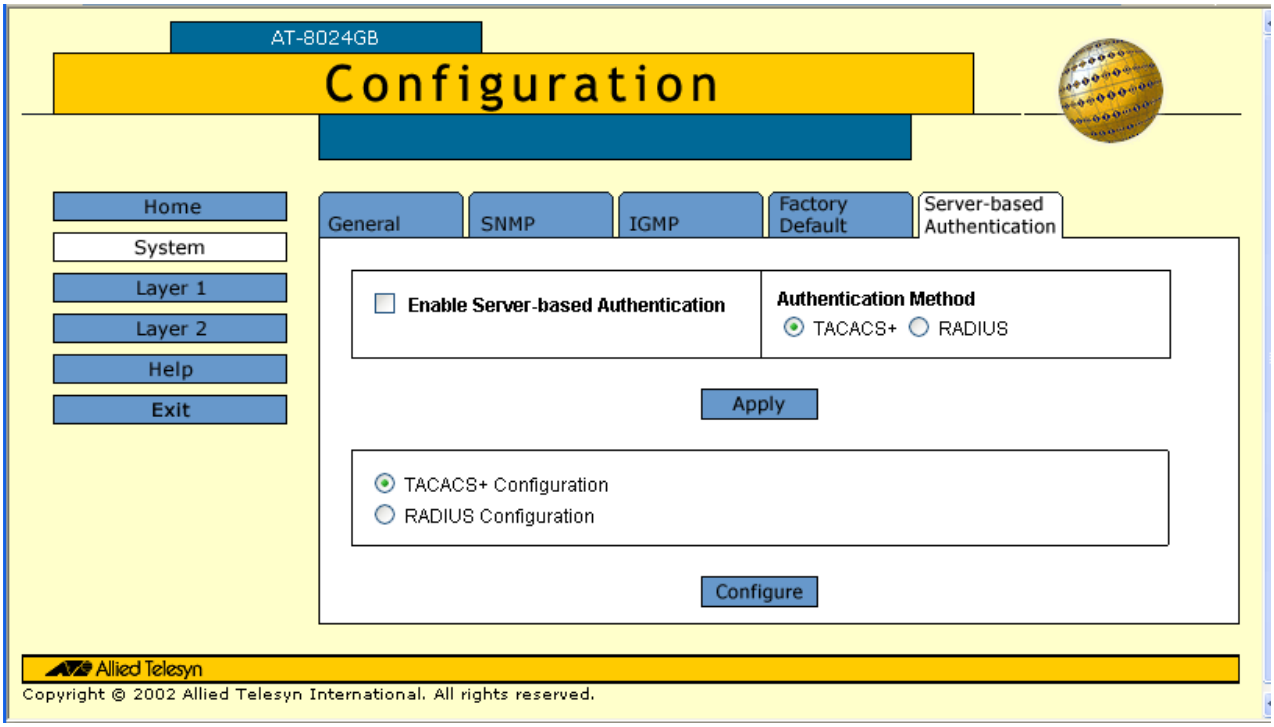

Figure 97 Server-based Authentication Tab

4. To enable or disable the authentication feature on the switch, click the Disable Server-based Authentication check box. A check in the box indicates that this feature is disabled. No check indicate the feature is enabled. The default is disabled.
5. To select an authentication protocol, click either TACACS+ or RADIUS in the Authentication Method section of the menu. The default is TACACS+.

> **Note**
> Only one authentication protocol can be active on the switch at a time.

6. Click **Apply**.

Note
If you activated the authentication feature, go to Step 6 to configure TACACS+ or Step 7 to configure RADIUS.

7. To configure TACACS+, do the following:

   a. From the Server-based Authentication tab, click the check circle next to TACACS+ Configuration and click **Configure**.

      The TACACS+ Configuration menu in Figure 98 is displayed.

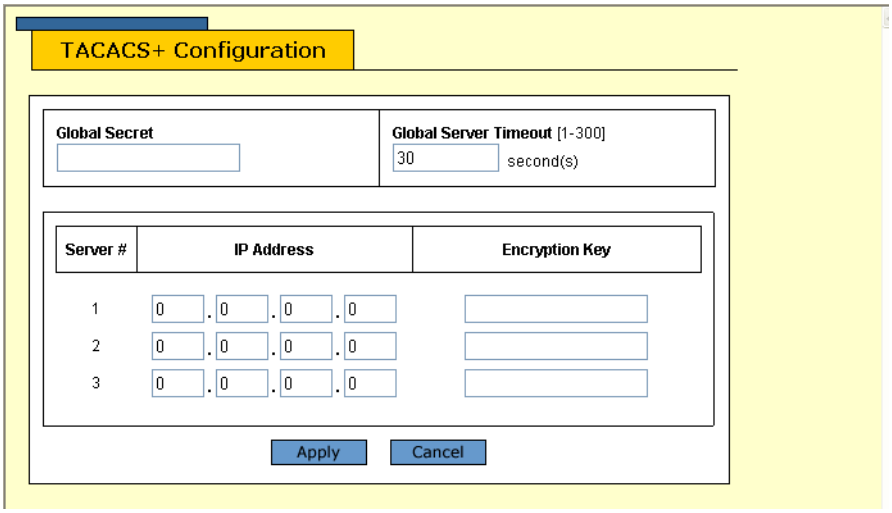

Figure 98 TACACS+ Configuration Menu

   b. Configure the parameters as needed. They are described below.

      Global Secret
      If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

      Global Server Timeout
      This parameter specifies the maximum amount of time the switch will wait for a response from a TACACS+ server before assuming the server cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there aren't any more servers, than the switch will default to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address and **Encryption Secret**
Use these fields to specify the IP addresses and encryption secrets of up to three network servers containing TACACS+ server software. You can leave an encryption field blank if you entered the server's secret in the Global Secret field.

c. After you have finished configuring the parameters, click **Apply**.

8. To configure RADIUS, do the following:

a. From the Server-based Authentication tab, click the check circle next to RADIUS Configuration and click **Configure**.

The RADIUS Configuration menu in Figure 98 is displayed.

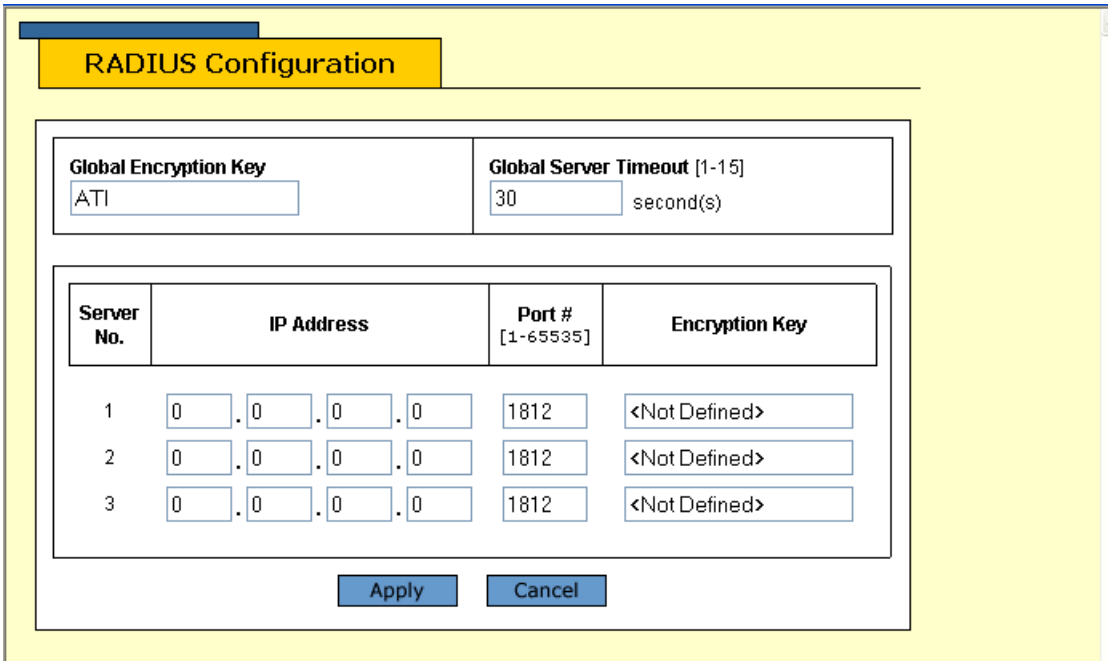

Figure 99 RADIUS Configuration

b. Configure the parameters as needed. They are described below.

Global Encryption Key
If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

Global Server Timeout
This parameter specifies the maximum amount of time the switch will wait for a response from a TACACS+ server before assuming the server cannot respond. If the timeout expires and the server has not responded, the switch

queries the next TACACS+ server in the list. If there aren't any more servers, than the switch will default to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address, Port #, and **Encryption Key**
Use these fields to specify the IP address, UDP port number, and encryption key of each RADIUS server. You can specify up to a maximum of three servers. You can leave the encryption field blank if you entered the server's key in the Global Secret field.

c. After you have finished configuring the parameters, click **Apply**.

Appendix A
AT-S39 Default Settings

This appendix lists the AT-S39 factory default settings.

Settings	Default
IP Address	0.0.0.0
Subnet Mask	255.255.0.0
Gateway Address	0.0.0.0
System Name	None
MAC Aging Time	300 seconds
Administrator's Comment	None
Switch Mode	Tagged
Console Disconnect Time	10 minutes
Web Server Status	Enabled
Console Startup Mode	Menu
Administrator's Comment	None
DHCP/BootP Status	Disabled
Default Web Access	Enabled
Default SNMP Access	Disabled
Console Menu Mode	Enabled
SNMP and Community Strings	
Get Community String	public
Set Community String	private
Trap Community String	public
SNMP Trap Receiver	Addr1
SNMP Trap Receiver	Addr2
SNMP Trap Receiver	Addr3

Settings	Default
SNMP Trap Receiver	Addr4
Server-Based Authentication	
Server Authentication	Disabled
Default Authentication Method	TACACS Plus
Spanning Tree Protocol	
Status	Disabled
Bridge Priority	32768
Bridge Max Age Time	20
Bridge Hello Time	2
Bridge Forwarding Delay	15
Port Costs	10 - 10 Mbps 10 - 100 Mbps 4 - 1000 Mbps
Port Priority	128
Fast Mode	No
Rapid Spanning Tree Protocol	
Status	Disabled
Bridge Priority	Increment 8 (32768)
Bridge Max Age Time	20
Bridge Hello Time	2
Bridge Forwarding Delay	15
Port Costs	Auto detect 2 000 000 - 10 Mbps 200 000 - 100 Mbps 20 000 - 1000 Mbps
Port Priority	Increment 8 (128)
Point-to-Point	Auto Detect
Edge Port	Yes
IGMP Snooping	
Status	Disabled
Topology	Single Host/ Port (Edge)
Host/Router Time-out Interval	260 seconds
Maximum Multicast Groups	256
Multicast Router Ports	Auto Detect
TACACS+ and RADIUS	
TACACS+	Disabled
RADIUS	Disabled

Settings	Default
TACACS Menu	
TACACS Timeout	30 seconds
Server IP 1	0.0.0.0
Server IP 2	0.0.0.0
Server IP 3	0.0.0.0
Server Key 1	0
Server Key 2	0
Server Key 3	0
RADIUS Menu	
Default Encryption Key	“ATI”
Server Timeout	30
Management Interface	
Manager Login Name (web browser session only)	manager
Manager Password	friend (case-sensitive)
Operator Login Name (web browser session only)	operator
Operator Password	operator (case-sensitive)
Time Out Value	10 minutes
Twisted Pair Ports	
Status	Enabled
Duplex Mode	Auto-negotiation
Speed	Auto-negotiation
Flow Control	Disabled
Broadcast Packets	Forwarded
Security	Automatic
VLANs	
Default_VLAN Name	Default_VLAN (all ports)
Ingress Filtering	Enabled
VLANs Mode	User Configured VLANs
VID	1
Basic Mode	Disabled
Broadcast Storm Control	
10/100 Mbps Interval Timer	10 milliseconds
1000 Mbps Interval Timer	100 microseconds
Maximum Number of Frames per Port	0 (disabled)

Settings	Default
Management Access	
Telnet	Enabled
Web	Enabled
SNMP	Disabled
Port Access Control	
Port Role	Authenticator
Port Control	Auto
Quiet Period	60 seconds
Tx Period	30 seconds
Reauth Period	3600 seconds
Supplicant Timeout	5 seconds
Server Timeout	30 seconds
Max Requests	10
RS232 Port	
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	Full-duplex
Data Rate	Auto-detect (default 9600 bps)

Index

802.1x port-based network access control
    configuring parameters, 204
    defined, 201
    enabling and disabling, 203
    overview, 200
    port access status, 207

A

Activating 158
aging time
    changing, 173, 295
    defined, 163
AT-S39 default settings, 54, 243, 312
AT-S39 software security, 48
AT-S39 software updates
    downloading from a local session, 216
    downloading from a Telnet session, 220
    obtaining, 215
AT-S39 switch modes, 116
AT-S39 version number, 52
authentication protocols, 192, 308
Automatic port security level, 76
Auto-Negotiation, 70, 251

B

Basic VLAN mode
    setting, 287
bootloader version number, 52
BOOTP
    activating, 42, 236
    defined, 42
BPDU, *see* bridge protocol data unit
bridge forwarding delay parameter, 107, 111, 269, 273
bridge hello time parameter, 107, 111, 269, 273
bridge identifier, 98, 112, 269, 274
bridge max age parameter, 107, 111, 269, 273
bridge priority, 98, 107, 111, 269, 273
bridge protocol data unit (BPDU), 107, 111, 269, 273
broadcast frame control
    configuring, 185, 304
    defined, 186
broadcast frames
    maximum number, configuring, 190, 306
browser tools, 229

C

cable detection
    configuring, 56
Class of Service
    configuring, 176, 297
    defined, 175
console timeout, 48

D

default values, AT-S39, 54, 243, 312
DHCP
    activating, 42, 236
    defined, 42
document conventions, 14
documentation, 15

E
enhanced stacking
changing switches, 63, 247
defined, 33, 37, 58
guidelines, 58
setting switch status, 61, 245

F
Fast Mode, 109
flow control, 71, 252
force version, 111, 273
forwarding delay, 101, 107

G
gateway address, 40, 235

H
hello time, 102, 107, 271
host nodes
defined, 178
displaying, 183, 302
host/router timeout interval, 181, 300

I
IEEE 802.1d standard, 106, 110, 268, 272
IGMP snooping
configuring, 180, 299
defined, 178
ingress filtering, 152
Internet Protocol (IP) address, 37, 40, 235
interval timer
configuring, 188, 305
defined, 186

L
limited security mode
configuring, 80
defined, 76
load distribution methods, 84
local management session
defined, 21
quitting, 33
starting, 29
Lock All Ports security level, 77

M
MAC address table, 161, 290
MAC address, switch, 52
management access levels, 25, 48
Management Information Base (MIB), 24
Manager access, 25, 48
Manager password, 48
master switch
assigning, 61, 245
defined, 61, 245
returning to, 64, 248
maxReq, 206
MDI/MDIX mode, 71, 252
MIBs, supported, 24
multicast groups, maximum, 181, 300
multicast MAC address
adding, 171, 293
deleting, 172, 294
displaying, 164
multicast router, displaying, 184, 302
multiple virtual LAN
802.1Q-compliant, 133
configuration, 156
defined, 132
mode
activating, 158
deactivating, 158
non-802.1Q compliant, 135

O
Operator access, 25, 48
Operator password, 48

P
password
changing, 40, 234
default, 31, 34, 228
pinging, 53, 242
port
configuring parameters, 69, 250
disable, 70, 251
displaying status, 66, 253
speed, 70, 251
statistics, 209, 256
port access control
configuring parameters, 204
enabling and disabling, 203
port access status, 207
port access control, 200

port access status
viewing, 207
port control
auto, 206
force-authorized, 205
force-unauthorized, 205
port control, 205
port cost
defined, 99
setting, 109, 113, 270, 275
port mirroring
creating, 94, 264
defined, 93
deleting, 95, 264
port role, 205
port security
configuring, 78
defined, 76
displaying, 259
port trunking
creating, 89, 261
defined, 83
deleting, 91, 261
guidelines, 83
load distribution methods, 84
port VLAN identifier (PVID)
defined, 122, 129
port-based VLAN
creating, 138, 142, 279, 285
defined, 121
deleting all, 150
deleting, 148, 283
displaying, 147, 160, 284
modifying, 144, 282
preserving user-configured VLAN definitions 157
priority queues, 175
priority, 109, 113, 271, 274

Q

quietPeriod, 206
quitting
local session, 33
Telnet session, 35
web browser session, 230

R

RADIUS
configuring, 195, 308
overview, 192
Rapid Spanning Tree Protocol
configuring port parameters, 112
reAuthPeriod, 206
resetting a switch, 47, 241
root bridge, 98
RS232 port, default settings, 30

S

Secure level, port security, 77
security
port access control, 200
serial number, switch, 52
serverTimeout, 206
setting the switch mode, 117
slave switch
assigning, 61, 245
defined, 61, 245
SNMP community strings, 44, 239
SNMP management session, 24, 48
snoop topology, 180, 300
software updates
downloading from a local session, 216
downloading from a Telnet session, 220
obtaining, 17, 215
Spanning Tree Protocol
configuring bridge parameters, 106, 110, 267
configuring port parameters, 108
defined, 97
port cost, 99, 109, 113, 270, 275
viewing bridge parameters, 276
starting session
local, 29
Telnet, 34
web browser, 228
static MAC address
adding, 171, 293
deleting, 172, 294
displaying, 164
statistics
port, 209, 256
switch, 211
STP. See Spanning Tree Protocol

subnet mask, 40, 235
suppTimeout, 206
switch mode
  configuring, 117
switch statistics, 211
system name, 40, 234

T
TACACS+
  configuring, 195, 308
  overview, 192
tagged VLAN
  creating, 138, 143, 279, 285
  defined, 127
  deleting all, 150
  deleting, 148, 283
  displaying, 147, 160, 284
  modifying, 144, 282
Telnet management session
  defined, 22
  quitting, 35
  starting, 34
TFTP, downloading and uploading files, 216, 220
txPeriod, 206

U
unavailable status, defined, 61, 245
user name, default, 228
user-configured VLAN
  defined, 121

V
version number, AT-S39, 52
virtual LAN
  creating, 138, 142, 143, 279, 285
  defined, 119
  deleting all, 150
  deleting, 148, 283
  disabling, 288
  displaying, 147, 160, 284
  enabling, 288
  mode, changing, 287
  modes, 120
  modifying, 144, 282
  multiple
    802.1Q-compliant, 133
    defined, 132
    non-802.1Q compliant, 135
  overview, 115
  port-based, defined, 121
  tagged, defined, 127
virtual LAN status
  setting, 118
VLAN identifier (VID), 122, 140, 145
VLAN identifier, 280
VLAN modes 120

W
web browser management session
  defined, 23
  disabling, 48
  limitations, 23
  quitting, 230
  starting, 228